Trials@uspto.gov
571-272-7822

Paper 42
Date: February 16, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
Petitioner,

v.

MYPORT, INC.,
Patent Owner.

IPR2023-00023 (Patent 9,832,017 B2)
IPR2023-00024 (Patent 10,237,067 B2)
IPR2023-00025 (Patent 10,721,066 B2)[1]

Before JEAN R. HOMERE, TERRENCE W. McMILLIN, and SEAN P. O'HANLON, *Administrative Patent Judges*.

O'HANLON, *Administrative Patent Judge*.

TERMINATION
Due to Settlement After Institution of Trial
35 U.S.C. § 317; 37 C.F.R. § 42.74

[1] This Order applies to each of the listed proceedings. The parties are not authorized to use this caption for any subsequent papers absent prior authorization from the Board.

I. INTRODUCTION

On February 15, 2024, with Board authorization (*see* Paper 39), Petitioner and Patent Owner filed a joint motion to terminate the above-captioned proceedings.[2] Paper 40 ("Mot."). Along with the motion, the parties filed a copy of a Confidential Settlement Agreement (Ex. 1037), as well as a joint request to treat the Confidential Settlement Agreement as business confidential information (Paper 41). *See* 37 C.F.R. § 42.74(c) ("A party to a settlement may request that the settlement be treated as business confidential information and be kept separate from the files of an involved patent or application.").

II. DISCUSSION

Under 35 U.S.C. § 317(a), "[a]n inter partes review instituted under this chapter shall be terminated with respect to any petitioner upon the joint request of the petitioner and the patent owner, unless the Office has decided the merits of the proceeding before the request for termination is filed." It is also provided in 35 U.S.C. § 317(a) that if no petitioner remains, the Office may terminate the *inter partes* review.

In each of these proceedings, the Board issued a decision to institute *inter partes* review. Paper 21. However, the Board has not yet decided the merits of the proceedings or entered final written decisions. In the joint motion, the parties state that they have settled their dispute and have reached an agreement to request termination of these *inter partes* reviews. Paper 40,

[2] Citations herein refer to documents filed in IPR2023-00023. Similar documents were filed in the other proceedings.

1–2. Accordingly, in the circumstances present here, we determine that it is appropriate to terminate the proceedings. 37 C.F.R. § 42.71(a). This Order does not constitute a final written decision pursuant to 35 U.S.C. § 318(a).

The parties also ask that the Confidential Settlement Agreement be treated as business confidential information and be kept separate from the file of the challenged patent. Paper 41. We determine that it is appropriate to treat the Confidential Settlement Agreement as business confidential information, and to keep that document separate from the files of the challenged patent, pursuant to 37 C.F.R. § 42.74(c).

III. ORDER

Accordingly, it is:

ORDERED that Joint Motion to Terminate (Paper 40) is *granted*;

FURTHER ORDERED that the Joint Request to treat the Confidential Settlement Agreement as business confidential information (Paper 41) is *granted*;

FURTHER ORDERED that the Confidential Settlement Agreement (Ex. 1037) shall remain designated as "Parties and Board Only" in the Board's electronic filing system, be kept separate from the files of the involved patent, and be made available only under the provisions of 35 U.S.C. § 317(b) and 37 C.F.R. § 42.74(c); and

FURTHER ORDERED that IPR2023-00023, IPR2023-00024, and IPR2023-00025 are *terminated*.

IPR2023-00023 (Patent 9,832,017 B2)
IPR2023-00024 (Patent 10,237,067 B2)
IPR2023-00025 (Patent 10,721,066 B2)

For PETITIONER:

Andrew R. Sommer
Jay Guiliano
Harry Park
Philip Hoffmann
Jenna Kuh
GREENBERG TRAURIG, LLP
sommera@gtlaw.com
jay.guiliano@gtlaw.com
parkh@gtlaw.com
hoffmannp@gtlaw.com
kuhj@gtlaw.com

For PATENT OWNER:

Matthew Phillips
Kevin Laurence
Derek Meeker
LAURENCE & PHILLIPS IP LAW
mphillips@lpiplaw.com
klaurence@lpiplaw.com
dmeeker@lpiplaw.com

John Lord
Sarah E. Spires
SKIERMONT DERBY LLP
jlord@skiermontderby.com
sspires@skiermontderby.com

Disclaimer

10,237,067 B2 - Michael F. Malone, McKinney, TX (US). APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSATION PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL/TAGS, STORAGE AND SEARCH RETRIEVAL. Patent dated March 19, 2019. Disclaimer filed January 24, 2023, by the assignee, MyPort, Inc.

I hereby disclaim the following complete claims 1-5 of said patent.

(Official Gazette, May 16, 2023)

Disclaimer

10,237,067 B2 - Michael F. Malone, McKinney, TX (US). APPARATUS FOR PERSONAL VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAG(S)/CONTEXTUAL TAG(S), STORAGE AND SEARCH RETRIEVAL. Patent dated March 19, 2019. Disclaimer filed January 24, 2023, by the inventor.

I hereby disclaim the following complete claims 1-5, of said patent.

(Official Gazette, May 2, 2023)

Trials@uspto.gov
571-272-7822

Paper 21
Date: April 24, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
Petitioner,

v.

MYPORT, INC.,
Patent Owner.

IPR2023-00024
Patent 10,237,067 B2

Before JEAN R. HOMERE, TERRENCE W. McMILLIN, and SEAN P. O'HANLON, *Administrative Patent Judges*.

O'HANLON, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Samsung Electronics Co., Ltd. ("Petitioner") filed a Petition for *inter partes* review of claims 1–17 of U.S. Patent No. 10,237,067 B2 (Ex. 1001, "the '067 patent"). Paper 1 ("Pet."), 1. MyPort, Inc. ("Patent Owner") filed a Preliminary Response. Paper 12 ("Prelim. Resp."). With our authorization (*see* Ex. 3002), Petitioner filed a Preliminary Reply (Paper 18, "Prelim. Reply") and Patent Owner filed a Preliminary Sur-reply (Paper 19, "Prelim. Sur-reply").

Institution of an *inter partes* review is authorized by statute only when "the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a) (2018). We have authority, acting on the designation of the Director, to determine whether to institute an *inter partes* review under 35 U.S.C. § 314 and 37 C.F.R. § 42.4(a). For the reasons set forth below, upon considering the parties' briefs and evidence of record, we conclude that the information presented shows that there is a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of at least one of the challenged claims. Thus, we institute *inter partes* review.

B. Real Parties in Interest

Petitioner identifies itself and Samsung Electronics America, Inc. as real parties in interest. Pet. 66.

Patent Owner identifies itself as the sole real party in interest. Paper 4, 2.

C. Related Matters

The parties indicate that the '067 patent is the subject of the following district court proceeding:

> *MyPort, Inc. v. Samsung Electronics Co., Ltd.*, Case No. 2:22-cv-114 (E.D. Tex. filed April 15, 2022) ("the Texas litigation").

Pet. 66; Paper 4, 2. The parties note other petitions for *inter partes* review filed by Petitioner and challenging patents owned by Patent Owner. Pet. 66; Paper 4, 2. More particularly, Petitioner filed a petition for *inter partes* review (IPR2023-00023) of claims 1–17 of U.S. Patent No. 9,832,017 and a petition for *inter partes* review (IPR2023-00025) of claims 1–17 of U.S. Patent No. 10,721,066. Pet. 66; Paper 4, 2.

D. The Challenged Patent

The '067 patent relates to the storage and retrieval of digital media files. Ex. 1001, 2:24–27. Digital media devices, such as mobile phones with audio and video recording capability, have greatly reduced the cost of creating new image, movie, and audio recordings, making the number of these recordings available in any given individual's library skyrocket. *Id.* at 2:31–40. This ability to store virtually unlimited numbers of media files, however, has created new problems. *Id.* at 2:41–42. For example, having a large number of media files increases the difficulty of manually describing and indexing the files. *Id.* at 2:42–44. Thus, "for many, photographs, movies and audio recordings are kept in poorly organized computer files and finding any particular picture, movie or recording is a difficult and time-consuming process." *Id.* at 2:44–48.

The '067 patent purports to provide an improved system having a capture device that includes a data converter for capturing various types of information, such as "[s]till pictures, moving pictures, audio, [and] telemetry," and organizing the information into a data element. Ex. 1001. 3:62–4:2. The data converter can be a digital camera, digital video recorder, or "any type of device that will capture the information and place it in some type of digitized format." *Id.* at 4:3–8. Metadata, such as time and date, location, operator identification, or other information relevant to establish the context of the data element, is created at the same time as the data element. *Id.* at 4:14–19. The capture device may also include a secondary data converter for gathering additional information that relates to defining the context of the data element. *Id.* at 4:35–38. "For example, after a camera/video recorder takes a picture/video, a microphone (the secondary data converter) might capture the audio describing the image or the audio from the video just captured." *Id.* at 4:38–42. This additional information is stored as a "context description element" with the data element and metadata. *Id.* at 4:42–43.

The capture device may send this stored data to a storage facility that may add "context tags," which are searchable elements derived from the different types of data. Ex. 1001, 5:10–14, 5:47–52. As an example, for a data element that "is a still photograph or video, the storage facility may create context tags that describe elements of the scene or image(s), such as 'animal,' or 'dog,' or 'Spot,' depending on the mechanism that converts the information in the data element or the context description element into a tag." *Id.* at 5:52–57. Context tags may be created using "a speech-to-text algorithm" for audio files or "image recognition and identification" for still

or moving images. *Id.* at 5:58–62. The result is a set of data for storage that "now includes a set of searchable tags specific to that image, video, audio or other media." *Id.* at 5:62–66.

Figure 2 illustrates "a diagrammatic view of the overall operation of the system," and is reproduced below. Ex. 1001, 6:43–44.

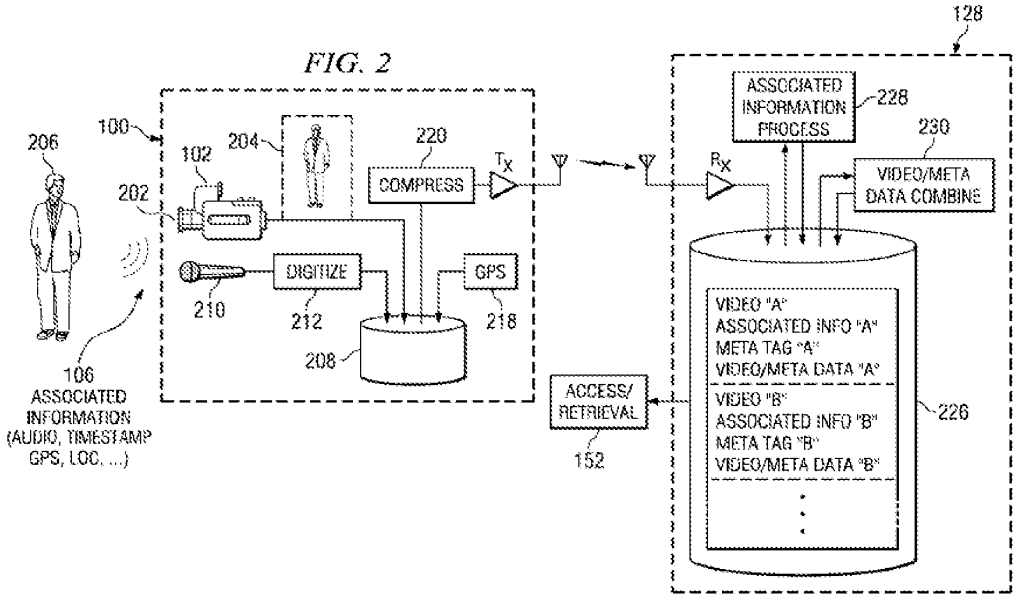


Figure 2 shows capture device system 100 including capture device 102, illustrated as a digital camera, and microphone 210. *Id.* at 6:43–59. All the information collected via the capture device and microphone is stored in database 208 within the capture device, from which location the information may be compressed and then sent to storage facility 128 for storage in database 226. *Id.* at 7:1–35. "At this time there will be, for example, a video clip or a video image (such as a still image) stored in association with the various information that is associated therewith." *Id.* at 7:37–40. Access and retrieval block 152 "can allow one to access the particular modified or 'tagged' image via a search," so that "[a]ny information that can be provided

over and above the video information that was provided in all of the associated information at the camera can then be searched." *Id.* at 7:62–8:4. In an alternative embodiment, illustrated in Figure 3, databases 208 and 226 are combined into a single database within the capture device, and the capture device creates and adds context tags to the image or video. *Id.* at 8:5–28; Fig. 3.

E. Disclaimer of Claims 1–5

A "patent owner may file a statutory disclaimer under 35 U.S.C. [§] 253(a) in compliance with § 1.321(a) of this chapter, disclaiming one or more claims in the patent. No *inter partes* review will be instituted based on disclaimed claims." 37 C.F.R. § 42.107(e). A disclaimer under 35 U.S.C. § 253(a) is "considered as part of the original patent" as of the date on which it is "recorded" in the U.S. Patent and Trademark Office ("Office"). 35 U.S.C. § 253(a). For a disclaimer to be "recorded" in the Office, the document filed by the patent owner must:

> (1) Be signed by the patentee, or an attorney or agent of record;
>
> (2) Identify the patent and complete claim or claims, or term being disclaimed. A disclaimer which is not a disclaimer of a complete claim or claims, or term will be refused recordation;
>
> (3) State the present extent of patentee's ownership interest in the patent; and
>
> (4) Be accompanied by the fee set forth in [37 C.F.R.] § 1.20(d).

37 C.F.R. § 1.321(a); *see also Vectra Fitness, Inc. v. TNWK Corp.*, 162 F.3d 1379, 1382 (Fed. Cir. 1998) (holding that a § 253 disclaimer is "recorded" on the date that the Office receives a disclaimer meeting the requirements of

37 C.F.R. § 1.321(a), and that no further action is required in the Office for a disclaimer to be "recorded").

Here, Patent Owner filed a statutory disclaimer of claims 1–5 of the '067 patent. Prelim. Resp. 8–9; Ex. 2002. Based on our review of Exhibit 2002, we determine that a disclaimer of claims 1–5 of the '067 patent under 35 U.S.C. § 253(a) has been filed with the Office as of January 24, 2023. Based on the information in the public record, we find that the disclaimer complies with the above-listed requirements of 37 C.F.R. § 1.321(a).

Because claims 1–5 have been disclaimed under 35 U.S.C. § 253(a), in compliance with 37 C.F.R. § 1.321(a), we do not reach challenges to claims 1–5. As a result, the remaining challenged claims are claims 6–17 ("the challenged claims").

F. The Challenged Claims

Petitioner challenges claims 6–17 of the '067 patent. Pet. 1. Claims 6 and 13 are independent. Claim 6 is illustrative of the challenged claims and is reproduced below.

> 6. A system for capturing image and audio information for storage, comprising:
>
> a capture device having:
>
> internal storage;
>
> a microphone interfaceable with [an] external audio information source that generates external audio information and a first data converter for capturing the first external audio information from the microphone,
>
> a camera interfacing with [an] external image source to capture an image therefrom;

the first data converter processing the captured external audio information and storing it in a first digital audio format as stored digital audio in internal storage within the capture device, the camera for processing the captured image and storing it as a stored digital image in internal storage;

a data capture device for capturing, as captured data, location information, and time information associated with at least the capture of the image and storing the captured data as stored captured data;

a media data converter for converting the the received digital audio to a text based searchable file as a text context tag and creating an image recognition searchable context tag with image recognition of at least a portion of the digital image and associating the text and image recognition context tags with the digital image and the captured data, and

the internal storage storing the digital image in association with the text and image recognition context tags in addition to the stored captured data.

Ex. 1001, 11:37–67.

G. Asserted Grounds of Unpatentability

The Petition relies on the following prior art references:

Name	Reference	Exhibit
Fuller	US 6,833,865 B1, issued December 21, 2004	1003
Rothschild	US 2006/0114338 A1, published June 1, 2006	1007
Anderson	US 6,499,016 B1, issued December 24, 2002	1008
Camahan	US 2005/0267894 A1, published December 1, 2005	1010
Davis	US 2002/0001395 A1, published January 3, 2002	1013

Petitioner asserts the following grounds of unpatentability:[1]

Claim(s) Challenged	35 U.S.C. §	Reference(s)
6–17	103(a)[2]	Rothschild, Anderson
6–9, 13–17	102(b)	Fuller
6–9, 13–17	103(a)	Fuller, Camahan
10–12	103(a)	Fuller, Davis
10–12	103(a)	Fuller, Camahan, Davis

Pet. 1. Petitioner submits a declaration of Benjamin B. Bederson, Ph.D. (Ex. 1002, "Bederson Declaration") in support of its contentions.

II. DISCRETIONARY DENIAL OF INSTITUTION

Under 35 U.S.C. § 314(a), the Director has discretion to deny institution. In determining whether to exercise that discretion on behalf of the Director, we are guided by the Board's precedential decision in *NHK Spring Co., Ltd. v. Intri-Plex Technologies, Inc.*, IPR2018-00752, Paper 8 (PTAB Sept. 12, 2018) (designated precedential).

In *NHK*, the Board found that the "advanced state of the district court proceeding" was a "factor that weighs in favor of denying" the petition under § 314(a). *NHK*, Paper 8 at 20. The Board determined that "[i]nstitution of an *inter partes* review under these circumstances would not be consistent with 'an objective of the AIA . . . to provide an effective and efficient alternative to district court litigation.'" *Id.* (citing *Gen. Plastic*

[1] A challenge to claims that Patent Owner has disclaimed (claims 1–5) is not listed here.

[2] The application resulting in the '067 patent claims priority to a date prior to the date when the Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112–29, 125 Stat. 284 (2011), took effect. Thus, we refer to the pre-AIA version of sections 102 and 103.

Indus. Co., Ltd. v. Canon Kabushiki Kaisha, IPR2016-01357, Paper 19 at 16–17 (designated precedential in relevant part)).

"[T]he Board's cases addressing earlier trial dates as a basis for denial under *NHK* have sought to balance considerations such as system efficiency, fairness, and patent quality." *Apple Inc. v. Fintiv Inc.*, IPR2020-00019, Paper 11 at 5 (PTAB Mar. 20, 2020) (designated precedential). *Fintiv* sets forth six non-exclusive factors for determining "whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding." *Id.* at 6. These factors are reproduced below:

> 1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
>
> 2. proximity of the court's trial date to the Board's projected statutory deadline for a final written decision;
>
> 3. investment in the parallel proceeding by the court and the parties;
>
> 4. overlap between issues raised in the petition and in the parallel proceeding;
>
> 5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
>
> 6. other circumstances that impact the Board's exercise of discretion, including the merits.

We discuss the parties' arguments in the context of considering the above factors. In evaluating the factors, we take a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review. *Fintiv*, Paper 11 at 6. We are also guided by the Director's Memorandum, *Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation*, issued

June 21, 2022 ("Guidance Memo"),[3] which provides several clarifications concerning the application of the *Fintiv* factors.

A. Whether the Court Granted a Stay or Evidence Exists that One May Be Granted if a Proceeding Is Instituted

The existence of a district court stay pending Board resolution of an *inter partes* review has weighed strongly against discretionary denial, while a denial of such a stay request sometimes weighs in favor of discretionary denial. *Fintiv*, Paper 11 at 6–8.

Patent Owner argues that this factor favors denial of institution because Petitioner has presented no evidence regarding a stay. Prelim. Resp. 52. According to Patent Owner, "a stay in [the Texas litigation] is extremely unlikely, as the [P]etitioner tacitly acknowledged when it chose not to file a reply brief in support of its stay motion." *Id.*

Petitioner replies that its "motion to stay remains pending." Prelim. Reply 4.

Patent Owner replies that Petitioner has failed to produce evidence that its motion to stay the Texas litigation will be granted if we institute review in this proceeding. Prelim. Sur-reply 1.

The record indicates that Petitioner has filed a motion to stay the Texas litigation (*see* Ex. 2011) and Patent Owner has filed an opposition to Petitioner's motion (*see* Ex. 2012). The likelihood of the district court

[3] *Available at* https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf.

granting Petitioner's motion is speculative. Accordingly, the facts underlying this factor are neutral.

B. Proximity of the Court's Trial Date to the Board's Projected Statutory Deadline for a Final Written Decision

When a district court's trial date will occur before the projected statutory deadline for the final written decision, the Board generally weighs this factor in favor of exercising discretion to deny institution. *Fintiv*, Paper 11 at 9. "If the court's trial date is at or around the same time as the projected statutory deadline or even significantly after the projected statutory deadline, the decision whether to institute will likely implicate other factors discussed herein, such as the resources that have been invested in the parallel proceeding." *Id.* When considering the facts underlying this factor, we "will consider the median time from filing to disposition of the civil trial for the district in which the parallel litigation resides." Guidance Memo 3. "[W]hen other relevant factors weigh against exercising discretion to deny institution or are neutral, the proximity to trial should not alone outweigh all of those other factors." *Id.* at 8. "Parties may present evidence regarding the most recent statistics on median time-to-trial for civil actions in the district court in which the parallel litigation resides for [our] consideration." *Id.* at 8–9 (footnote omitted).

Petitioner acknowledges that "trial [in the Texas litigation] is . . . about six weeks before an anticipated final written decision," but argues that "trial dates are unpredictable, and the median time to trial in the Eastern District of Texas is 24.5 months, placing trial more than a month after a [final written decision], thus favoring institution." Pet. 65 (citing Ex. 1023; Guidance Memo 3, 8–9).

Patent Owner argues that this factor favors denial because "the [Texas litigation] is scheduled to begin two months and three weeks *before* the final written decision would be due in this case." Prelim. Resp. 52 (citing *id.* at 11; Ex. 2013, 1). Patent Owner argues that Petitioner's calculation of the projected trial date is incorrect and asserts that the median time of 24.5 months puts the trial date "just two business days after the [final written decision] deadline." *Id.* at 53. Continuing, Patent Owner argues that "the median time to trial has been skewed recently because of the coronavirus pandemic," and that, prior to the pandemic, "the median time to trial in the U.S. District Court for the Eastern District of Texas was only 17.5 months." *Id.* (citing Ex. 1023, 35).

Petitioner replies that "the Director's [Guidance] Memo accounted for [delays due to the coronavirus pandemic] when stating that the Office would rely on median times to trial." Prelim. Reply 5.

Patent Owner replies that "nothing in the [Guidance] Memo condones reliance on skewed statistics." Prelim. Sur-reply 1.

The latest statutory due date for a final written decision in this proceeding is April 26, 2024. The Texas litigation is scheduled to begin on February 5, 2024. Ex. 2013, 1. However, Petitioner presents evidence that, as of June 30, 2022, the median time-to-trial for civil actions in the Eastern District of Texas is 24.5 months (Ex. 1023, 35), which, as Patent Owner concedes, would place the trial date two days after the latest statutory due date for a final written decision in this proceeding (Prelim. Resp. 53). The most recent statistics show that, as of December 31, 2022, the median time-to-trial date for civil actions in the Eastern District of Texas is 19.0 months

(Ex. 3003, 35), which would place the trial date prior to the February 5, 2024, scheduled date.

Accordingly, the facts underlying this factor weigh in favor of exercising our discretion to deny institution. However, the Guidance Memo instructs us that, "when analyzing the proximity of the court's trial date under factor two of *Fintiv*, when other relevant factors weigh against exercising discretion to deny institution or are neutral, the proximity to trial should not alone outweigh all of those other factors." Guidance Memo 8.

C. Investment in the Parallel Proceeding by the Court and the Parties

If, at the time of the institution decision, the district court has issued substantive orders related to the challenged patent, such as a claim construction order, this fact weighs in favor of denial. *See Fintiv*, Paper 11 at 9–10. On the other hand, if the district court has not issued such orders, this fact weighs against discretionary denial. *Id.* at 10. Additionally, we also consider Petitioner's diligence in filing the Petition in weighing this factor. *Fintiv*, Paper 11 at 11 ("If the evidence shows that the petitioner filed the petition expeditiously, such as promptly after becoming aware of the claims being asserted, this fact has weighed against exercising the authority to deny institution under *NHK*.").

Petitioner argues that "the parties and court have not significantly invested in the case because fact discovery is, at best, in its infancy, invalidity contentions are not due for a month, and this Petition is being filed within a month of receiving infringement contentions, thus favoring institution." Pet. 65–66.

Patent Owner argues that, "[b]y the time the decision on institution is due in this case, the parties and the court will have invested significant time and energy in the case including, for example, exchange of infringement and invalidity contentions, engaging in fact discovery, and beginning the claim construction process." Prelim. Resp. 53.

Petitioner replies that Patent Owner "has not identified any efforts it has made to litigate the validity issue, which is the relevant question under *Fintiv* factor 3." Prelim. Reply 5 (citing *Sand Revolution II, LLC v. Cont'l Intermodal Grp.–Trucking LLC*, IPR2019-01393, Paper 24 at 11–12 (PTAB June 16, 2020) (designated informative)).

Patent Owner replies that, "[b]y the time the decision on institution is made, the parties will have served invalidity contentions; engaged in fact discovery regarding, *inter alia*, validity; and begun the claim construction process, which affects validity and overlaps with the IPR." Prelim. Sur-reply 1.

In the Texas litigation, the parties have exchanged infringement and invalidity contentions. Ex. 2013, 4; Ex. 2004. Claim construction does not appear to be an issue, as the parties have not sought construction of any term in this proceeding. *See generally* Prelim. Resp.; Pet. 2. Fact and expert discovery, expert reports, dispositive motions, and, if applicable, claim construction briefing will continue well after the Institution Decision deadline. Ex. 2013, 2–5. Thus, the parties have engaged in some work in the Texas litigation, but significant work still remains to be done.

Patent Owner filed its complaint in the Texas litigation on April 15, 2022. Ex. 1015, 35. Petitioner diligently filed its Petition on October 11, 2022 (Paper 3, 1), approximately one month after Patent Owner filed its

infringement contentions (*see* Ex. 2013, 4) and six months prior to the statutory deadline for filing the Petition (*see* 35 U.S.C. § 315(b)).

Accordingly, the facts underlying this factor weigh against exercising our discretion to deny institution.

D. Overlap Between Issues Raised in the Petition and in the Parallel Proceeding

"[I]f the petition includes the same or substantially the same claims, grounds, arguments, and evidence as presented in the parallel proceeding, this fact has favored denial." *Fintiv*, Paper 11 at 12. "Conversely, if the petition includes materially different grounds, arguments, and/or evidence than those presented in the district court, this fact has tended to weigh against exercising discretion to deny institution under *NHK*." *Id.* at 12–13.

Concerns about the degree of overlap may be mitigated where a petitioner agrees not to pursue in the parallel district court litigation the grounds advanced in the petition. *Sand Revolution*, IPR2019-01393, Paper 24 at 11–12. The Board suggested that a broader stipulation such as one stipulating that the petitioner "would not pursue any ground raised or that could have been reasonably raised in an IPR, i.e., any ground that could be raised under §§ 102 or 103 on the basis of prior art patents or printed publications" would better address concerns relating to overlapping issues. *Id.* at 12 n.5; *see also* Guidance Memo 7 (explaining that such a broad stipulation obviates a full analysis of the *Fintiv* factors).

Petitioner concedes that the Petition includes the same or substantially the same claims, grounds, arguments, and evidence as it presents in the Texas litigation. Prelim. Reply 5 (asserting that Petitioner "will withdraw its contentions *based on the grounds it has presented in the Petition* in the

[Texas] litigation" (emphasis added)). However, Petitioner's stipulation reduces the overlap relating to the challenges presented in the Petition and mitigates "to some degree the concerns of duplicative efforts between the district court and the Board, as well as concerns of potentially conflicting decisions." *See Sand Revolution*, IPR2019-01393, Paper 24 at 12.

Accordingly, the facts underlying this factor weigh marginally against exercising our discretion to deny institution.

E. Whether the Petitioner and the Defendant in the Parallel Proceeding Are the Same Party

"If a petitioner is unrelated to a defendant in an earlier court proceeding," this fact has weighed against exercising discretion to deny institution. *Fintiv*, Paper 11 at 13–14.

There is no dispute that the parties in this proceeding are identical to the parties in the Texas litigation. *See* Prelim. Resp. 58; Pet. 66. Thus, the facts underlying this factor are neutral.

F. Merits and Other Circumstances that Impact the Board's Exercise of Discretion

Petitioner argues that this factor favors institution because its "Petition presents a strong case of unpatentability." Pet. 66.

Patent Owner argues that "this factor definitely points toward denial" because "of the substantial flaws in the [P]etition's challenges." Prelim. Resp. 58. Patent Owner argues that "the relative size and stature of the parties also weighs in favor of denial," asserting that "[P]etitioner has nearly one-quarter of a million employees worldwide and annual revenue over $225 billion, whereas [Patent Owner] is a single-employee company." *Id.*

Patent Owner asserts that Petitioner has a "strategy of filing multiple IPR petitions timed such that major deadlines in the IPRs would coincide or interfere with major deadlines in the [Texas] litigation." *Id.* Finally, Patent Owner argues that "there is limited public interest in the validity of the '067 Patent." *Id.* at 59.

Petitioner replies that Patent Owner's description of its challenge to claims 6–17 based on the combination of Rothschild and Anderson ("Challenge 2") as being flawed is incorrect, making several assertions as to why Patent Owner's arguments regarding the merits of Challenge 2 are unpersuasive. Prelim. Reply 1–2. Petitioner makes similar arguments regarding its challenges to claims 6–17 that use Fuller as the primary asserted reference, again making arguments responsive to Petitioner's criticisms of the merits of Patent Owner's challenges. *Id.* at 3–4. Additionally, Petitioner replies that the Texas litigation is funded by an investor. *Id.* at 5 (citing Ex. 1028).

Patent Owner replies that Petitioner's "Reply uses almost four of its five pages to respond to [Patent Owner's Preliminary Response] arguments against the merits of the challenges," which "exceeds the scope of the additional briefing requested by the [P]etitioner and granted by the Board." Prelim. Sur-reply 2–3.

As a preliminary matter, we agree that Petitioner's arguments regarding the merits of its challenges are outside the authorized scope of the Preliminary Reply. In our communication authorizing the additional briefing, we instructed the parties that "[t]he [Preliminary] Reply is limited . . . to addressing the *Fintiv* issues identified by Petitioner below." Ex. 3002, 1. Petitioner identified those issues as "Patent Owner's positions

on *Fintiv* factors 1-4 and 6, and Patent Owner's 'additional considerations' related to *Fintiv*." *Id.* Petitioner's arguments regarding the merits of its challenges exceed the allowed scope for the Preliminary Reply, and we therefore do not consider such unauthorized arguments.

Petitioner presents five grounds challenging the '067 patent, with three of its challenges addressing the independent claims. Pet. 1. For reasons provided below, we find that Petitioner establishes a reasonable likelihood of prevailing on two of these challenges. As discussed in more detail below, we find the evidence and arguments presented by Petitioner for these challenges persuasive on this preliminary record and sufficient to meet our standard for instituting *inter partes* review. For the reasons provided below, however, we are not persuaded that Petitioner establishes a reasonable likelihood of prevailing on its other challenge to the independent claims.

Patent Owner's assertions regarding Petitioner's "strategy" of filing petitions for *inter partes* review (*see* Prelim. Resp. 58–59) is speculative and, therefore, unavailing.

Accordingly, the facts underlying the merits of Petitioner's challenges to the '067 patent claims are neutral.

G. Holistic Assessment of the *Fintiv* Factors

On this record, after weighing all of the factors and taking a holistic view, we determine that the facts in this case that weigh against exercising discretion outweigh the facts that favor exercising discretion. Accordingly, we determine that the circumstances presented weigh against exercising our

discretion under 35 U.S.C. § 314(a) to deny institution of *inter partes* review based on the Texas litigation.

Additionally, given that our analysis of the first five *Fintiv* factors does not favor exercising our discretion to deny institution, we need not consider whether the Petition presents a compelling, meritorious challenge. *Commscope Techs., LLC v. Dali Wireless, Inc.*, IPR2022-01242, Paper 23 at 4–5 (PTAB Feb. 27, 2023) (designated precedential).

III. PATENTABILITY ANALYSIS

A. Principles of Law

1. Inter Partes *Review*

"In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify "with particularity . . . the evidence that supports the grounds for the challenge to each claim")). Petitioner bears the burden of persuasion to prove unpatentability of each challenged claim by a preponderance of the evidence. 35 U.S.C. § 316(e). This burden never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). The Board may authorize an *inter partes* review if we determine that the information presented in the Petition and Patent Owner's Preliminary Response shows that there is a reasonable likelihood that Petitioner will prevail with respect to at least one of the claims challenged in the petition. 35 U.S.C. § 314(a).

2. Anticipation

"Under 35 U.S.C. § 102 a claim is anticipated 'if each and every limitation is found either expressly or inherently in a single prior art reference.'" *King Pharm., Inc. v. Eon Labs, Inc.*, 616 F.3d 1267, 1274 (Fed. Cir. 2010) (quoting *Celeritas Techs. Ltd. v. Rockwell Int'l Corp.*, 150 F.3d 1354, 1360 (Fed. Cir. 1998)). "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Therasense, Inc. v. Becton, Dickinson & Co.*, 593 F.3d 1325, 1332 (Fed. Cir. 2010) (quoting *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548 (Fed. Cir. 1983)).

A reference inherently discloses an element of a claim "if that missing characteristic is necessarily present, or inherent, in the single anticipating reference." *Schering Corp. v. Geneva Pharm.*, 339 F.3d 1373, 1377 (Fed. Cir. 2003) (citing *Cont'l Can Co. USA, Inc. v. Monsanto Co.*, 948 F.2d 1264, 1268 (Fed. Cir. 1991)). "Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing *may* result from a given set of circumstances is not sufficient." *Therasense*, 593 F.3d at 1332 (quoting *Cont'l Can*, 948 F.2d at 1269).

3. Obviousness

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying

factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) when in evidence, any objective evidence of nonobviousness.[4] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

The level of ordinary skill in the art is "a prism or lens" through which we view the prior art and the claimed invention. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). The person of ordinary skill in the art is a hypothetical person presumed to have known the relevant art at the time of the invention. *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). In determining the level of ordinary skill in the art, we may consider certain factors, including: "(1) the educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of active workers in the field." *Best Med. Int'l, Inc. v. Elekta Inc.*, 46 F.4th 1346, 1353 (Fed. Cir. 2022) (citations omitted). "The patent's purpose can also be informative." *Id.*

Petitioner contends that a person having ordinary skill in the art at the time of the invention "would have had a Bachelor's degree in electrical engineering, computer engineering, computer science, or a related field and two years of practical experience in technologies involved with categorizing media including images and applying metadata to such images." Pet. 7

[4] At this stage of the proceeding, the parties have not directed us to any such objective evidence.

(citing Ex. 1002 ¶¶ 3–19, 33). Petitioner asserts that such an artisan would have had "familiarity with software for automatically generating metadata from audio and images (*e.g.*, speech-to-text and image recognition)," performed "work done in ensuring associations were maintained between metadata and images," and "standardized techniques for associating metadata with images and various known data 'container' formats." *Id.* (citing Ex. 1002 ¶¶ 12, 33).

Patent Owner does not contest Petitioner's proffered definition of the level of ordinary skill in the art or offer a definition of its own. *See generally* Prelim. Resp.

We find Petitioner's description to be consistent with the problems and solutions disclosed in the '067 patent and prior art of record, and adopt it as our own for purposes of this Decision. *See, e.g.*, *In re GPAC Inc.*, 57 F.3d at 1579 (approving the determination of the level of ordinary skill in the art by appeal to the references of record).

C. Claim Construction

In an *inter partes* review, claims are construed using the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b), including construing the claims in accordance with the ordinary and customary meaning of such claims as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b). "[T]he ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention" and "after reading the entire patent." *Phillips v. AWH Corp.*, 415

F.3d 1303, 1313, 1321 (Fed. Cir. 2005) (en banc). In addition to the specification and prosecution history, we also consider use of the terms in other claims and extrinsic evidence including expert and inventor testimony, dictionaries, and learned treatises, although extrinsic evidence is less significant than the intrinsic record. *Id.* at 1312–17. Usually, the specification is dispositive, and it is the single best guide to the meaning of a disputed term. *Id.* at 1315.

"The Board is required to construe 'only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.'" *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (alteration in original) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Petitioner contends that "[n]o formal claim constructions are needed." Pet. 2.

Patent Owner does not propose a definition for any claim term. *See generally* Prelim. Resp.

For purposes of this Decision, and based on the record before us, we determine that no construction of any term is necessary. We note that this determination does not preclude the parties from arguing their proposed constructions of the claims during trial. Indeed, the parties are hereby given notice that claim construction, in general, is an issue to be addressed at trial. A final determination as to claim construction will be made at the close of the proceeding, after any hearing, based on all the evidence of record.

D. Overview of the Asserted Prior Art

1. Rothschild

Rothschild relates to "devices, systems and methods for embedding and retrieving information in digital images and using the information to organize, process and control the digital images." Ex. 1007 ¶ 3. Rothschild recognizes that cataloging photographs manually is an extensive process that requires a significant amount of time, and that this problem has been exacerbated by the advent of digital cameras. *Id.* ¶¶ 5–6. Rothschild purports to improve upon the prior art by providing a system and method of organizing, controlling, and manipulating digital images. *Id.* ¶ 9.

Rothschild discloses a device, such as a digital camera or mobile phone, for capturing images. Ex. 1007 ¶¶ 25, 42. Figures 1A and 1B illustrate an embodiment of the device and are reproduced below.

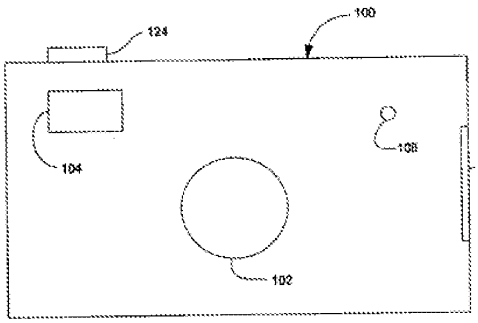


FIG. 1A

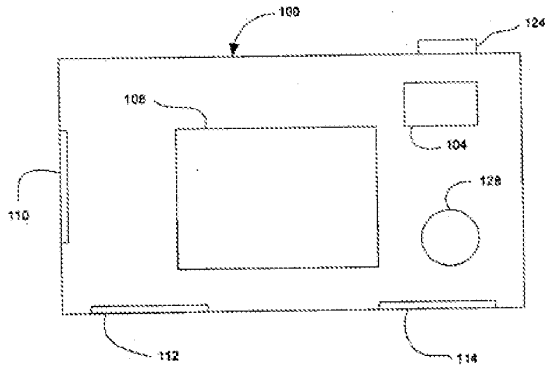


FIG. 1B

Figures 1A and 1B show front and rear views, respectively, of device 100. *Id.* ¶¶ 25–26. The device includes lens 102 for use in capturing an image, viewfinder 104, and "microphone 106 for acquiring audio, from the user of the device or from the subject of the image, which may be associated with

the image." *Id.* ¶ 25. Display module 108 displays a captured image and facilitates "user input of information to be associated with a digital image." *Id.* ¶ 26. The device also includes "storage module 110 for storing a plurality of images" and "transmission module 112 for transmitting the plurality of images to another device." *Id.*

In use, the device user takes several pictures. Ex. 1007 ¶ 47. A capture module captures the images. *Id.* ¶ 29. The capture module includes an analog-to-digital (A/D) converter that converts the images into digital form. *Id.* The digital images may be processed, such as by enhancing and compressing the images, and the processed images are stored in a storage module. *Id.* The user can enter information about the images using an input module. *Id.* ¶ 47. The input module accepts user input via touch screen that overlays display module 108 or via microphone 106. *Id.* ¶ 31. The microphone may be coupled to an A/D converter that converts the user's spoken audio information into a digital format. *Id.* Furthermore, the input module may include a voice recognition processor that translates the digital human voice into alpha numeric characters for user input. *Id.* For example, for a picture of the user's "baby in Las Vegas," the user may "record an audio file indicating: 'this is a picture of my baby girl Samantha here in Las Vegas. Boy is she cute.'" *Id.* ¶¶ 47, 49. The device obtains time and date information, user identification information, and the number of the digital image, and stores this information with the audio file either as a separate information file associated with the image or appended to the digital image file. *Id.* ¶¶ 51–52.

The images and associated files are then transferred to the user's computer, which sorts and stores the images and associated information in

the location specified by the user. Ex. 1007 ¶¶ 53–54. The computer parses the associated information and stores the data in a relational database. *Id.* ¶ 63, Fig. 7. The computer may be used to print an image with symbology that encodes the location of the associated information. *Id.* ¶ 39. The device can be scanned over the printed image to read the symbology and retrieve the associated information. *Id.* ¶ 57. This allows, for example, the device to retrieve and play the audio file. *Id.* ¶ 58.

The device may include a user verification module for verifying an identity of the device user. Ex. 1007 ¶ 33. The user verification module may include an identify capture device, such as a facial recognition reader. *Id.* The identity capture device collects information from the user and compares the collected information to information that has previously been stored in the device memory. *Id.* For example, the capture module may capture an image of the user's face, which may then be processed by a facial recognition algorithm executed by the user verification module. *Id.*

2. Anderson

Anderson relates to categorizing, storing and presenting digital images. Ex. 1008, 2:42–43. Anderson's system allows "a user to categorize images at the time of capture with multiple categories of information by merely speaking into the camera." *Id.* at 2:16–19. "[T]he user's voice annotations are automatically recognized, translated, and stored in a database . . . ." *Id.* at 2:19–22. Figure 1 illustrates an exemplary system and is reproduced below.

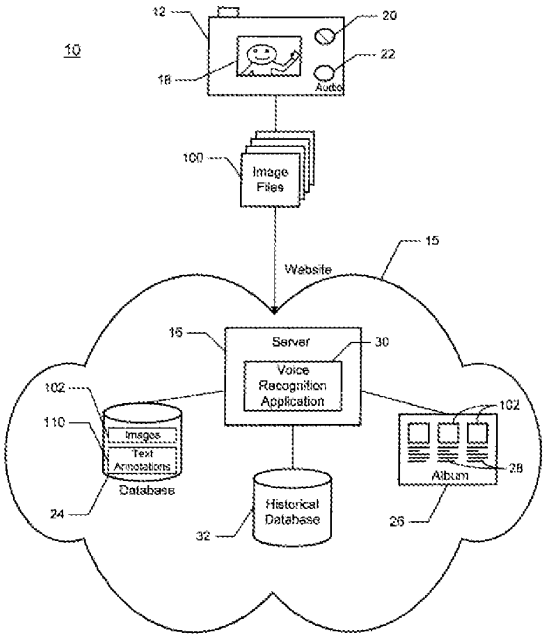


FIG. 1

Figure 1 shows system 10, including digital camera 12 for capturing digital images. *Id.* at 2:56–57. The digital camera includes microphone 20 and audio button 22 for recording sound. *Id.* at 2:58–61. A user may upload image files 100 to website 15, where web server 16 includes voice recognition application 30 and database 24. *Id.* at 2:61–65. In use, a user may record category-specific voice annotations on the digital camera, which "are then translated by voice recognition into text annotations." *Id.* at 3:10–15. An image and its corresponding text annotations are stored and indexed in database 24 "so that the images may be found more easily." *Id.* at 3:15–19.

3. Fuller

Fuller relates to the automatic extraction of metadata descriptions of digital multimedia content such as still images and video. Ex. 1003,

2:53–55. Figure 1 illustrates "a generic digital capture system . . . combined with an embedded, real-time, content-based analysis engine and data output" and is reproduced below. *Id.* at 4:49–52.

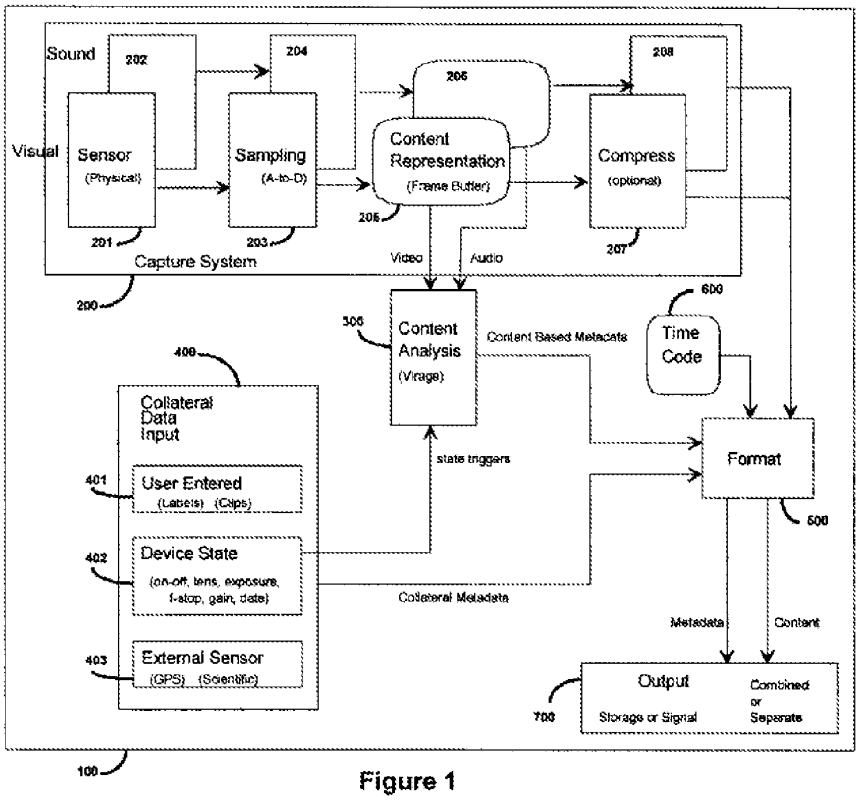


Figure 1

Figure 1 shows the overall system architecture digital capture system 100, which includes visual and audio capture subsystem 200, content-based metadata generation engine 300, collateral data gathering block 400, data formatting unit 500 with optional time code marking 600, and data output and/or storage 700. *Id.* at 5:23–29.

Visual and audio capture subsystem 200 may include visual sensor 201 and microphone 202. Ex. 1003, 5:32–34. The output from these sensors is converted to digital form and may be filtered by analog-to-digital

units 203 (visual), 204 (audio), and the digital content is stored in memory units 205, 206, respectively. *Id.* at 5:34–38. The digital content may then optionally be compressed prior to being formatted at unit 500 for output or storage. *Id.* at 5:38–42.

Content-based analysis engine 300 accesses the digital representation of visual and audio content from memory units 205, 206 and extracts metadata from the content. Ex. 1003, 5:43–45. The engine performs "sophisticated analysis of multimedia content and generate[s] metadata descriptions that can be effectively used to index the content for downstream applications such as search and browse." *Id.* at 2:58–62. The content-based analysis engine may be "the Virage audio and video engines" that "are further described in U.S. [P]atent [A]pplication[] . . . No. 09/134,500" (Ex. 1005, "the '500 application"). *Id.* at 7:53–59. This engine includes a speech transcription module that processes speech and that may output recognized keywords or the full text of the transcription process, which may be used directly as metadata. Ex. 1005, 15:24–16:9.[5]

Collateral data gathering block 400 gathers various forms of collateral metadata (metadata that is not based on the content), including user-provided information at block 401, device state information at block 402, and external sensor information at block 403. Ex. 1003, 5:49–57. "Content-based metadata from the analysis engine 300 is joined by collateral metadata (not based on the digital content) from block 400 in the formatting unit 500." *Id.* at 5:58–60. The metadata and related digital content may be combined or stored separately. *Id.* at 6:13–34.

[5] We cite to the application pagination rather than the exhibit pagination.

4. Camahan

Camahan relates to "a metabase specifically designed for the organization, management and manipulation of digital media assets." Ex. 1010 ¶ 2. Camahan's metabase is "a collection of node objects which can be implemented as XML elements and organized in a tree-like or hierarchical structure that emanates from a single root node, and stored in disk drive storage or internal cache storage." *Id.* ¶ 90. In the metabase, a "folder represents a generic container," and "[e]ach folder 201 may contain child folders 205, 207, 209 allowing the metabase to be organized in a hierarchy similar to a conventional file system." *Id.* ¶ 92; *see also id.* at Fig. 2. Further, a folder "may also contain one or more binders," where each binder "represents a media asset within the metabase and 'binds' together all of the metadata related to that asset." *Id.* ¶ 96. A binder, in turn, may contain "one or more content objects each describing a different aspect . . . of the media asset." *Id.* ¶ 100. For example, "[a] label object 211 contains structured metadata that describes the entire media asset such as the title, rating, author, etc.," and "[a] track object 213 contains structured metadata that occur at specific points or during specific intervals within the media asset such as closed captions, key frames, or speech-to-text extraction." *Id.* ¶¶ 104, 107.

5. Davis

Davis relates to associating "data with a media signal by encoding the data, a link to the data, or a combination of both into the media signal." Ex. 1013, code (57). Davis's system associates data in images or other media signals using steganographic and other techniques. *Id.* ¶ 24. The

data, which may describe, for example, objects in the image or the context of the image, can be encoded within the image or stored elsewhere. *Id.* ¶¶ 15–23, 25. For example, the image can be uploaded to an image database and the metadata can be uploaded to a metadata database. *Id.* ¶ 89. Alternatively, the metadata can be stored in a database integrated with the image database. *Id.* ¶ 173.

E. Asserted Obviousness Based on Rothschild and Anderson

Petitioner argues that claims 6–17 would have been obvious in view of Rothschild and Anderson. Pet. 29–43. In support of its showing, Petitioner relies upon the Bederson Declaration. *Id.* (citing Ex. 1002). We have reviewed Petitioner's assertions and supporting evidence. For the reasons discussed below, and based on the record before us, we are not persuaded that Petitioner demonstrates a reasonable likelihood of prevailing in showing that at least one challenged claim would have been obvious in view of the combination of Rothschild and Anderson.

Independent claim 6 recites, in relevant part, "a media data converter for converting the the received digital audio to a text based searchable file as a text context tag." Ex. 1001, 11:58–60. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:51–52. Petitioner maps Rothschild's input module 124, auxiliary input computer module 126, and user verification module 132, collectively, to the recited media data converter. Pet. 34. Petitioner argues that "Rothschild's input module includes [a] voice recognition processor that converts speech to text" and "Rothschild's user input data can be stored as a file associated with the captured image." *Id.* at 34–35 (citing Ex. 1007 ¶ 32; Ex. 1002 ¶ 182).

Petitioner asserts that "[t]ext derived from voice recognition is a text context tag because . . . it is a searchable element derived from a context description element (*i.e.*, speech 'regarding the pictures')." *Id.* at 35 (citing Ex. 1007 ¶ 47; Ex. 1002 ¶¶ 135, 161). Petitioner relies on "Jim Jones," shown in Figure 7, as an example of a context tag. *Id.* Continuing, Petitioner argues that it would have been obvious to an ordinarily skilled artisan "to use Rothschild's input module to convert received digital audio to a text based searchable file as a text context tag because doing so would allow for descriptive information to be associated with the image for later search and retrieval using a text-based search query . . . as taught by Anderson." *Id.* (citing Ex. 1002 ¶¶ 185–186, 179–180).

Patent Owner refers to this challenge as "challenge 2" and the challenge to disclaimed claims 1–5 as "challenge 1," and argues that Rothschild does not disclose converting a digital audio file into a text-based searchable file. Prelim. Resp. 29–38. First, Patent Owner argues that "[t]he [P]etition does not clearly identify what is the 'external audio information' or corresponding 'stored digital audio.'" *Id.* at 29. Patent Owner asserts that "[i]t appears that the [P]etition and Dr. Bederson assume that the 'external audio information' in challenge 2 is the same as in challenge 1." *Id.* at 31 (citing Ex. 1002 ¶ 171). Patent Owner argues that this mapping of the recited external audio information fails because "there is no disclosure in Rothschild that the user of the camera speaks in association with the user-verification selfie." *Id.* at 29; *see also id.* at 31 (stating that "there is no indication in Rothschild that the user . . . speaks his name (or anything else) to the camera in connection with user verification" and "Rothschild does *not* disclose voice recognition as a user-verification technique").

Rothschild discloses a user entering information via voice recognition software regarding pictures taken by the user. Ex. 1007 ¶ 47. However, Petitioner does not map these "pictures" to the recited image. Rather, Petitioner relies on an image of the device user taken for verifying the user's identity. Pet. 30–31 (citing Ex. 1007 ¶ 33). For the recited audio information, Petitioner relies on its showing made for challenge 1 (*id.* at 30), in which Petitioner maps "audio 'from the user of the device or from the subject of the image'" to the recited audio information (*id.* at 13 (citing Ex. 1007 ¶¶ 25, 31, 42, 49, Figs. 1A, 1B, 3A, 3B)). Thus, the Petition relies on audio acquired from the user or subject (*id.*) that is first converted to digital form (*id.* at 14) and then converted to text (*id.* at 34–35). But this audio is not associated with the user verification image, which the Petition maps to the recited image. *Id.* at 30–31. Neither Petitioner nor its declarant appears to explain adequately how Rothschild discloses a user entering speech regarding the user verification image. Thus, Rothschild does not appear to support Petitioner's assertions.

Independent claim 6 also recites, in relevant part, "a media data converter for . . . creating an image recognition searchable context tag with image recognition of at least a portion of the digital image." Ex. 1001, 11:58–62. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:51–55. Petitioner argues that Rothschild's user verification module 132 "uses facial recognition to identify users of the device and then stores a tag associated with that user—*e.g.*, 'John Jones' (*see* FIG. 7) to associate it with images captured by that user." Pet. 37 (citing Ex. 1007 ¶¶ 33, 66, 83–84). Petitioner argues that "[t]he user's name is an image recognition context tag because it is derived from an image." *Id.*

Patent Owner argues that "nothing in Rothschild states or implies that the name of the recognized individual in the user-verification image is used as 'an image recognition searchable context tag.'" Prelim. Resp. 39. Patent Owner argues that "Rothschild does not disclose that a user image taken for user verification is treated like all the other images." *Id.*

Petitioner's mapping of the recited image here ("images captured by that user" (Pet. 37)) is different than and incompatible with Petitioner's prior mapping of the recited image ("an image of the face of the user" (*id.* at 31)). Thus, Petitioner appears to fail to explain adequately how Rothschild supports its contentions.

Additionally, neither Petitioner nor its declarant appears to explain adequately how Rothschild stores the user's name in association with the verification picture. Rothschild discloses that its "user verification module 132 will indicate and verify the identity of the user of the device 100 at the time of the image capture." Ex. 1007 ¶ 33. This verification may use a "facial recognition reader" that "will collect information on the user to be compared to information that has previously been stored in the device's memory." *Id.* "[C]apture module 122 may capture am image of the face of the user which may then be processed by a facial recognition algorithm executed by the user verification module 132." *Id.* However, Rothschild does not appear to disclose storing a context tag associated with that user's verification image as asserted by Petitioner. *See* Pet. 37. Petitioner's reference to Rothschild's locational image verification device to transmit the user's name in association with a photograph taken by the user (*id.* (citing Ex. 1007 ¶¶ 83–84)) also fails to explain adequately how a tag is associated with the user verification image.

For at least these reasons, we question whether Petitioner demonstrates a reasonable likelihood of prevailing in showing that independent claims 6 and 13 and their dependent claims 7–12 and 14–17 would have been obvious in view of Rothschild and Anderson.

F. Assertions Based on Fuller

Petitioner argues that claims 6–9 and 13–17 are anticipated by Fuller or are rendered obvious based on the combined teachings of Fuller and Camahan. Pet. 43–60. In support of its showing, Petitioner relies upon the Bederson Declaration. *Id.* (citing Ex. 1002). We have reviewed Petitioner's assertions and supporting evidence. For the reasons discussed below, and based on the record before us, we are persuaded that Petitioner demonstrates a reasonable likelihood of prevailing in showing that at least one challenged claim is anticipated by Fuller or rendered obvious in view of Fuller and Camahan.

1. The Preamble

Independent claim 6 recites "[a] system for capturing image and audio information for storage." Ex. 1001, 11:37–38. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:33–34. Petitioner argues that Fuller discloses such a system because it stores digital media content and metadata. Pet. 44 (citing Ex. 1003, 4:23–34, 5:22–25, 8:35–37, Fig. 6).

Patent Owner does not contest this aspect of the Petition. *See generally* Prelim. Resp.

Fuller discloses a digital capture system that includes a visual and audio capture subsystem. Ex. 1003 5:23–28.

Accordingly, for the foregoing reasons and on this record, to the extent the preamble is limiting, Fuller supports Petitioner's contentions.

2. The Capture Device Recitation

Independent claim 6 recites "a capture device." Ex. 1001, 11:39. Independent claim 13 does not contain a substantially similar recitation. Ex. 1001, 12:33–60. Petitioner maps Fuller's digital capture system to the recited capture device. Pet. 44 (citing Ex. 1003, 4:49–52, 5:22-41, code (57). Fig. 1; Ex. 1002 ¶ 206).

Patent Owner does not contest this aspect of the Petition. *See generally* Prelim. Resp.

Fuller discloses a digital capture system that includes a visual and audio capture subsystem. Ex. 1003 5:23–28.

Accordingly, for the foregoing reasons and on this record, Fuller supports Petitioner's contentions.

3. The Storage Recitation

Independent claim 6 recites "internal storage." Ex. 1001, 11:40. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:35. Petitioner maps Fuller's memory units 205, 206, storage 700, and internal storage unit 702, collectively, to the recited internal storage. Pet. 44–45 (citing Ex. 1003 5:23–28, 5:34–38, 6:23–31, 7:35–38, 8:8–12; Ex. 1002 ¶ 207).

Patent Owner does not contest this aspect of the Petition. *See generally* Prelim. Resp.

Fuller discloses that its digital capture system 100 stores digital visual data in memory unit 205, stores digital audio data in memory unit 206, and

stores formatted digital content in storage 700. Ex. 1003 5:36–40. In an embodiment of a video camera capture device, storage 700 is referred to as internal storage unit 702. *Id.* at 8:8–10, Fig. 4.

Accordingly, for the foregoing reasons and on this record, Fuller supports Petitioner's contentions.

4. The Microphone Recitation

Independent claim 6 recites "a microphone interfaceable with [an] external audio information source that generates external audio information and a first data converter for capturing the first external audio information from the microphone." Ex. 1001, 11:41–45. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:36–39. Petitioner maps Fuller's microphone 202 to the recited microphone and analog-to-digital unit 204 to the recited first data converter. Pet. 45 (citing Ex. 1003, 5:29–35, 7:34–37; Ex. 1002 ¶ 208).

Patent Owner does not contest this aspect of the Petition. *See generally* Prelim. Resp.

Fuller's digital capture system 100 includes "a microphone 202 if audio is being captured." Ex. 1003, 5:32–34. Fuller discloses that the output of microphone 202 is converted to digital form by analog-to-digital unit 204. *Id.* at 5:34–36.

Accordingly, for the foregoing reasons and on this record, Fuller supports Petitioner's contentions.

5. The Camera Recitation

Independent claim 6 recites "a camera interfacing with [an] external image source to capture an image therefrom." Ex. 1001, 11:46–47.

Independent claim 13 contains a substantially similar recitation. *Id.* at 12:40–41. Petitioner maps Fuller's digital capture system to the recited camera, noting that it may include visual sensor 201. Pet. 46 (citing Ex. 1003, 4:49–51, 5:29–32, 7:31–34, 8:16–18; Ex. 1002 ¶¶ 210–211).

Patent Owner does not contest this aspect of the Petition. *See generally* Prelim. Resp.

Fuller's digital capture system 100 includes visual and audio capture subsystem 200, which includes visual sensor 201 that captures images. Ex. 1003, 5:30–34, 7:33–35.

Accordingly, for the foregoing reasons and on this record, Fuller supports Petitioner's contentions.

6. The First Data Converter Recitation

Independent claim 6 recites "the first data converter processing the captured external audio information and storing it in a first digital audio format as stored digital audio in internal storage within the capture device." Ex. 1001, 11:48–51. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:46–48. Petitioner argues that Fuller's analog-to-digital unit 204 "processes the captured external audio information by digitizing it" and "stores the captured external audio information in internal storage in the capture device by outputting it to a 'sound buffer 206.'" Pet. 47 (citing Ex. 1003, 5:35–37, 7:40–43, 7:51, Figs. 1, 4–5; Ex. 1002 ¶ 212).

Patent Owner first argues that Petitioner fails to show the recited processing in Fuller. Prelim. Resp. 45–46. According to Patent Owner, "[w]hile Fuller does teach that 'audio is captured by a microphone 202,' that is digitized audio that is captured." *Id.* at 46 (citing Ex. 1003, 7:34–35).

Fuller's microphone 202 captures audio information in the form of sound waves, analog-to-digital unit 204 processes the captured sound into digital format, and memory 206 stores the digitized content. Ex 1003, 5:30–38, 7:35–38. The "digitization of signals from the microphone" noted by Patent Owner (*see* Prelim. Resp. 45) is the "processing." *See* Pet. 47. Petitioner's mapping of digitization to the recited processing is consistent with the processing disclosed in the '067 patent. *See, e.g.*, Ex. 1001, 6:56–59 ("One method for collecting the audio information, for example, is to utilize a microphone 210 that will capture the information and then digitize it in a digitizing block 212 utilizing an analog-to-digital converter, for example.").

Next, Patent Owner argues that Fuller does not disclose storing audio information in a first digital audio format. Prelim. Resp. 47–48. Patent Owner acknowledges that Fuller discloses digitizing audio information "in 'a sequence of 8-bit or 16-bit waveform samples at a suitable sampling frequency, such as 44.1 kHz (for CD quality audio),'" but argues that this "is not a disclosure of 'a first digital audio format.' Quite to the contrary, such a sequence of samples is just that – a sequence of samples, sans any format." *Id.* at 47 (quoting Ex. 1003, 7:40–43).

As noted above, Fuller discloses that its analog-to-digital unit 204 converts the captured audio information into digital form and stores it in memory unit 206. Ex. 1003, 5:30–38. We understand Fuller's disclosure of "digital form" to be equivalent to a digital format. Indeed, it is difficult to envision how digital audio information can be stored in memory if it is not in some digital format. That Fuller might not disclose explicitly what that format is does not indicate that there is no such format.

Accordingly, for the foregoing reasons and on this record, Fuller supports Petitioner's contentions.

7. The Processing Recitation

Independent claim 6 recites "the camera for processing the captured image and storing it as a stored digital image in internal storage." Ex. 1001, 11:51–53. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:49–50. Petitioner argues that Fuller's analog-to-digital unit 203 converts the output of visual sensor 201 into digital form and "[t]he digitized image 'is then stored in a memory unit 205." Pet. 47–48 (citing Ex. 1003, 5:31–38, 7:33–40, Figs. 1, 4; Ex. 1002 ¶ 213).

Patent Owner does not contest this aspect of the Petition. *See generally* Prelim. Resp.

The output of Fuller's visual sensor 201 is converted into digital form by analog-to-digital unit 203 and the digitized content is stored in memory 205. Ex 1003, 5:30–38.

Accordingly, for the foregoing reasons and on this record, Fuller supports Petitioner's contentions.

8. The Data Capture Device Recitation

Independent claim 6 recites "a data capture device for capturing, as captured data, location information, and time information associated with at least the capture of the image and storing the captured data as stored captured data." Ex. 1001, 11:54–57. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:42–45. Petitioner maps Fuller's collateral data gathering block 400 to the recited data capture device and argues that "it is used to capture 'collateral metadata' such as 'time/date' and

'position derived from GPS satellites.'" Pet. 48 (citing Ex. 1003, 4:15–20, 5:22–28, 5:49–57, Fig. 1; Ex. 1002 ¶ 214). Petitioner argues that the captured data "is joined with content-based metadata in the formatting unit 500" and "then stored in storage 700." *Id.* at 49 (citing Ex. 1003, 5:58–6:22, 6:23–27, 8:1–10, 8:35–9:47, Fig. 6; Ex. 1002 ¶ 215).

Patent Owner does not contest this aspect of the Petition. *See generally* Prelim. Resp.

Fuller discloses that collateral data gathering block 400 gathers collateral metadata including device state information such as "time/date" and external sensor information such as "position derived from GPS satellites." Ex. 1003, 5:49–57. "Content-based metadata from the analysis engine 300 is joined by collateral metadata . . . from block 400 in the formatting unit 500." *Id.* at 5:58–60. The metadata and related digital content may be combined or stored separately. *Id.* at 6:13–34.

Accordingly, for the foregoing reasons and on this record, Fuller supports Petitioner's contentions.

9. The Converting Recitation

Independent claim 6 recites "a media data converter for converting the the received digital audio to a text based searchable file as a text context tag." Ex. 1001, 11:58–60. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:51–52. Petitioner maps Fuller's content-based analysis engine 300 to the recited second data converter and argues that it includes "the 'Virage Audio Engine' described in the incorporated '500 application." Pet. 50 (citing Ex. 1003, 2:53–3:8, 5:43–60, 7:51–59, 8:16–18, 8:51–55, Figs. 1, 4–5; Ex. 1002 ¶ 217). Petitioner argues that the

'500 application discloses that the audio engine includes audio analysis feature extractor 516, which

> classifies audio input as "speech," passes the audio signal to "a speech transcription module" that interfaces "with any available Speech Recognition Engine 624" . . . , and uses a "Keyword Spotting Feature Extractor 640" to "selectively identify keywords of interest and produce a text output 648 limited to the keywords specified by a Domain Dictionary 642."

Id. at 50–51 (citing Ex. 1005, 15:6–7, 15:14–16:9, Figs. 9–10).[6] Petitioner asserts that "[t]he resulting text defines text tags including full text or keywords" that are "stored in a text-based searchable file which contains 'tracks' of metadata." *Id.* at 51 (citing Ex. 1005, 11:1–3, 11:12; Ex. 1002 ¶ 219). Petitioner also argues that the text is searchable because Fuller discloses that "the 'content-based signal analysis' is 'added to a metadata batch under construction.'" *Id.* at 52 (citing Ex. 1003, 2:53–62, 8:45–57; Ex. 1002 ¶ 220).

Petitioner also relies on Camahan to provide additional teaching regarding text context tags. Pet. 58–60. Petitioner argues that Camahan teaches "storing text-based tracks in searchable XML files." *Id.* at 58. Petitioner argues that Camahan discloses a metabase of node objects, one such object being a binder that includes track objects that contain structured metadata such as speech-to-text extractions stored as searchable XML files. *Id.* at 58–59 (citing Ex. 1010 ¶¶ 90, 96, 102, 107–108, 155; Ex. 1002 ¶ 239). Petitioner argues that it would have been obvious to an ordinarily skilled

[6] On pages fifty to fifty-one of the Petition, Petitioner's first citation to Exhibit 1005 refers to the exhibit pagination and Petitioner's second citation refers to the application pagination. For consistency and ease of reading, we convert Petitioner's citations to the application pagination.

artisan to store Fuller's keyword tracks as searchable XML files because "Fuller expressly suggests doing so" and "files were known data containers for metadata." *Id.* at 59 (citing Pet. 54–55; Ex. 1010 ¶ 155; Ex. 1002 ¶ 240). Petitioner also argues that the proposed modification "would have merely been the simple substitution of Fuller's tracks for a track defined as a .xml file using conventional techniques that were accessible to the [ordinarily skilled artisan]." *Id.* at 60 (citing Ex. 1002 ¶ 242).

Patent Owner first argues that "Fuller does not teach that the output of the analysis engines 300 or 301 is a file" and that "the '500 application teaches that the output of the extractor 516 is full text or keywords, not files." Prelim. Resp. 43–44 (citing Ex. 1003, 6:24–28, 6:66–7:2, Fig. 3; Ex. 1005, 15:6–16:17, Fig. 10).

Patent Owner's arguments are not availing. The '500 application discloses that its audio analysis feature extractor passes digitized speech data to a speech transcription module that interfaces with a speech recognition engine and outputs the full text of the transcription process, which may be used directly as metadata. Ex. 1005, 15:6–16:3. Alternatively, the output can be limited to keywords recognized in the text. *Id.* at 16:3–5. The '500 application discloses that "the metadata may be output in a variety of formats such as Virage Data Format (VDF) 562, HTML 564, XML 566, SMIL 568 and other 570." *Id.* at 13:26–28. Moreover, Fuller discloses that that the metadata extracted by the engines is used for search and browse functions. *See, e.g.*, Ex. 1003, 2:53–62.

Regarding the obviousness challenge based on Fuller and Camahan, Patent Owner acknowledges that "Camahan discloses XML files," but argues that "the tracks relied on by the [P]etition are not described as files."

Prelim. Resp. 49 (citing Ex. 1010 ¶¶ 153–157, 170). According to Patent Owner, "a track is just data, not a file." *Id.*

As explained above, Petitioner relies on Camahan to teach "storing [Fuller's] text-based tracks in searchable XML files." Pet. 58. Patent Owner's arguments do not address the combination of Fuller and Camahan as set forth in the Petition. Moreover, as noted above, Fuller, through the '500 application, discloses storing metadata in XML files. Ex. 1005, 13:26–28.

Accordingly, for the foregoing reasons and on this record, Fuller and the combination of Fuller and Camahan support Petitioner's contentions. We determine that Petitioner sets forth reasoning with rational underpinning as to why a person having ordinary skill in the art would have combined the teachings of Fuller and Camahan. *See* Pet. 59–60.

10. The Creating Recitation

Independent claim 6 recites the "media data converter for . . . creating an image recognition searchable context tag with image recognition of at least a portion of the digital image." Ex. 1001, 58, 60–62. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:51, 53–55. Petitioner argues that Fuller's content-based analysis engine 300 performs metadata extraction from the digital image through face and character recognition and produces a searchable context tag for the image based on the extracted metadata. Pet. 52–53 (citing Ex. 1003, 1:59–64, 2:53–3:8, 5:35–36, 5:43–45, 5:58, 8:45–57; Ex. 1002 ¶ 224).

Patent Owner does not contest this aspect of the Petition. *See generally* Prelim. Resp.

Fuller discloses that its content-based analysis engine 300 accesses the digital representation of visual content from memory unit 205 to perform metadata extraction. Ex. 1003, 5:43–45. The generated metadata is used for search and browse functions, and may include face identification/recognition and optical character recognition. *Id.* at 2:58–3:8.

Accordingly, for the foregoing reasons and on this record, Fuller supports Petitioner's contentions.

11. The Associating Recitation

Independent claim 6 recites the "media data converter for . . . associating the text and image recognition context tags with the digital image and the captured data." Ex. 1001, 58, 62–64. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:51, 55–57. Petitioner argues that Fuller's content-based analysis engine 300 "joins the content-based metadata with the captured data (*i.e.*, Fuller's 'collateral metadata') in the 'formatting unit 500'" in MPEG-7 format. Pet. 54 (citing Ex. 1003, 5:56–6:12, 8:1–5).

Patent Owner does not contest this aspect of the Petition. *See generally* Prelim. Resp.

Fuller discloses that "[c]ontent-based metadata from the analysis engine 300 is joined by collateral metadata (not based on the digital content) from block 400 in the formatting unit 500." Ex. 1003, 5:58–60. The metadata and related digital content may be combined in a variety of formats, including MPEG-7. *Id.* at 6:13–31.

Accordingly, for the foregoing reasons and on this record, Fuller supports Petitioner's contentions.

12. The Storing Recitation

Independent claim 6 recites "the internal storage storing the digital image in association with the text and image recognition context tags in addition to the stored captured data." Ex. 1001. 11:65–67. Independent claim 13 contains a substantially similar recitation. *Id.* at 12:58–60. Petitioner argues that Fuller discloses storing the combined metadata and image MPEG-7 file in internal storage unit 702. Pet. 55 (citing Ex. 1003, 6:13–14, 8:8–18, Figs. 1, 4; Ex. 1002 ¶ 228).

Patent Owner does not contest this aspect of the Petition. *See generally* Prelim. Resp.

Fuller discloses that "[t]he formatted output data of the formatting unit 500 can be handled by the output system 700 in a variety of ways," including combing the metadata and actual digital content in MPEG-7 format and storing the file in internal memory. Ex. 1003, 6:13–31.

Accordingly, for the foregoing reasons and on this record, Fuller supports Petitioner's contentions.

13. Conclusion Regarding Independent Claims 6 and 13

For the foregoing reasons, we determine that Petitioner has established a reasonable likelihood of prevailing on its assertion that independent claims 6 and 13 are anticipated by Fuller and would have been obvious in view of the combination of Fuller and Camahan.

IV. CONCLUSION

For the foregoing reasons, we determine that the information presented establishes a reasonable likelihood that Petitioner would prevail in

showing that at least one challenged claim of the '067 patent is unpatentable. At this preliminary stage, we have not made a final determination with respect to the patentability of the challenged claims or any underlying factual and legal issues. *See TriVascular, Inc. v. Samuels*, 812 F.3d 1056, 1068 (Fed. Cir. 2016) (noting that "there is a significant difference between a petitioner's burden to establish a 'reasonable likelihood of success' at institution, and actually proving invalidity by a preponderance of the evidence at trial").

Accordingly, *inter partes* review is instituted as to all challenged, non-disclaimed claims and all proposed grounds of unpatentability. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1354, 1359–60 (2018); *see also PGS Geophysical AS v. Iancu*, 891 F.3d 1354, 1360 (Fed. Cir. 2018) (interpreting the statute to require "a simple yes-or-no institution choice respecting a petition, embracing all challenges included in the petition"); Patent Trial and Appeal Board Consolidated Trial Practice Guide 64 (Nov. 2019)[7] ("The Board will not institute on fewer than all claims or all challenges in a petition.").

V. ORDER

ORDERED that pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 6–17 of the '067 patent is instituted with respect to all grounds set forth in the Petition; and

[7] *Available at* https://www.uspto.gov/TrialPracticeGuideConsolidated.

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial, which commences on the entry date of this decision.

For PETITIONER:

Andrew R. Sommer
Jay Guiliano
Harry Park
Philip Hoffmann
Jenna Kuh
GREENBERG TRAURIG, LLP
sommera@gtlaw.com
jay.guiliano@gtlaw.com
parkh@gtlaw.com
hoffmannp@gtlaw.com
kuhj@gtlaw.com

For PATENT OWNER:

Matthew Phillips
Kevin Laurence
Derek Meeker
LAURENCE & PHILLIPS IP LAW
mphillips@lpiplaw.com
klaurence@lpiplaw.com
dmeeker@lpiplaw.com

John Lord
Sarah E. Spires
SKIERMONT DERBY LLP
jlord@skiermontderby.com
sspires@skiermontderby.com

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/824,087	11/28/2017	Michael F. Malone	MPOR60-33823

CONFIRMATION NO. 5197

25883
MUNCK WILSON MANDALA L.L.P
P.O. Drawer 800889
DALLAS, TX 75380

POWER OF ATTORNEY NOTICE

OC000000137314006

Date Mailed: 02/06/2023

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/23/2023.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/atesfai/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/824,087	11/28/2017	Michael F. Malone	MYPT.01.01.US7

CONFIRMATION NO. 5197

40672
LAW OFFICE OF BILL NAIFEH
PO BOX 803423
DALLAS, TX 75380

POA ACCEPTANCE LETTER

OC000000137314018

Date Mailed: 02/06/2023

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/23/2023.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/atesfai/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No. **10,237,067**	
Title: APPARATUS FOR PERSONAL VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAG(S)/CONTEXTUAL TAG(S), STORAGE AND SEARCH RETRIEVAL	
Inventor: Michael F. Malone	Confirmation No. 5197
Filing Date: 2017 November 28	Examiner: Ishrat I. Sherali
Attorney Docket No. MPOR60-33823	Group Art Unit: 2667

TRANSMITTAL FOR STATUTORY DISCLAIMER

A statutory disclaimer of the above-referenced patent is being filed herewith. The disclaimer is signed by the Michael F. Malone, CEO of MyPort, Inc., who is authorized to make the disclaimer. A declaration attesting to his authority accompanies the disclaimer.

The $170 fee as required by 37 C.F.R. § 1.20(d) is being paid herewith.

Respectfully submitted,

Date: January 24, 2023

/Bill R. Naifeh, Reg. No. 44,962/

Registration No. 44,962

Bill R. Naifeh
Law Office of Bill Naifeh
13155 Noel Road, Suite 900
Dallas, TX 75240
972-726-9500
214-550-2542 (fax)

STATUTORY DISCLAIMER UNDER 37 C.F.R. § 2.321(a)

MyPort, Inc. hereby disclaims claims 1-5 of U.S. Patent No. 10,237,067.

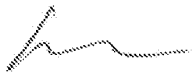
MyPort, Inc. is the owner of 100% interest in the above-referenced patent, as reflected by assignments recorded as follows: Reel 044493, frame 0702; reel 045082, frame 0529; and reel 059507, frame 0960.

Date: 1-27-23

Michael F. Malone
CEO, MyPort, Inc.

DECLARATION REGARDING AUTHORITY TO SIGN ON BEHALF OF A LEGAL ENTITY

Pursuant to 37 C.F.R. § 3.73(d)(1), I, Michael F. Malone, hereby declare that I am authorized to signed documents on behalf of MyPort, Inc.



Date: 1-25-03

Michael F. Malone
CEO, MyPort, Inc.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
15/824,087	01/24/2023 02:22:24 PM ET	MPOR60-33823

Title of Invention

APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL TAGS, STORAGE AND SEARCH RETRIEVAL

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	10237067
CONFIRMATION #	5197	FILED BY	April Reasoner
PATENT CENTER #	61483610	AUTHORIZED BY	Bill Naifeh
CUSTOMER #	25883	FILING DATE	11/28/2017
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Michael F. Malone

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 2001	E20231NE23184991	April Reasoner

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
1814	STATUTORY DISCLAIMER, INCLUDING TERMINAL DISCLAIMER	170.00	1	170.00
			TOTAL AMOUNT:	$170.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d)

and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
15/824,087	**01/24/2023 02:22:24 PM ET**	**MPOR60-33823**

Title of Invention

APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL TAGS, STORAGE AND SEARCH RETRIEVAL

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	10237067
CONFIRMATION #	5197	FILED BY	April Reasoner
PATENT CENTER #	61483610	FILING DATE	11/28/2017
CUSTOMER #	25883	FIRST NAMED INVENTOR	Michael F. Malone
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Bill Naifeh

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
Statutory-Disclaimer-10237067.pdf	3	Statutory disclaimers per Manual of Patent Examining Procedure(MPEP) 1490.	502 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
Statutory-Disclaimer-10237067.pdf	F8863EFDEA25E9E7975D60AD69CE949E18F179B068023F76F7D81CCF6E1BB7B5E66108BF62D7D4436BACFCBE017E0A8E3

1FB5A35511972191FAF0784EB53350F

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
15/824,087	**01/23/2023 07:16:02 PM ET**	**MPOR60-33823**

Title of Invention

APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL TAGS, STORAGE AND SEARCH RETRIEVAL

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	10237067
CONFIRMATION #	5197	FILED BY	April Reasoner
PATENT CENTER #	61479661	FILING DATE	11/28/2017
CUSTOMER #	25883	FIRST NAMED INVENTOR	Michael F. Malone
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Bill Naifeh

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
POA-Statement_10237067.pdf	3	Power of Attorney	1552 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
POA-Statement_10237067.pdf	3BDEFE4CAF0444B2FF3E9B65EF658C6460460EAE20759118A58EACA9F212B08F9990E454FC3E985A07FC112699D0B5A6DE82FD73C09B3BA280AAD81CCDABD2E2

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized

by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/81A (02-15)
Approved for use through 03/31/2021. OMB 0651-0035
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

PATENT - POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Patent Number	10237067
Issue Date	03/19/2019
First Named Inventor	Michael F. Malone
Title	APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL TAGS, STORAGE AND SEARCH RETRIEVAL
Attorney Docket No.	MYPT.01.01.US7

I hereby revoke all previous powers of attorney given in the above-identified patent.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the Customer Number identified in the box at right as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

40672

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified patent to:

☒ The address associated with the above-identified Customer Number.

OR

☐ The address associated with the Customer Number identified in the box at right:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the:

☐ Applicant.

OR

☒ Patent owner.

Statement under 37 CFR 3.73(c) (Form PTO/AIA/96) submitted herewith or filed on _____

SIGNATURE of Applicant or Patent Owner

Signature		Date	1-23-23
Name	Michael F. Malone	Telephone	
Title and Company	CEO of MYPORT, INC.		

NOTE: Signatures of all the applicants or patent owners of the entire interest or their representative(s) are required. If more than one signature is required, submit multiple forms, check the box below, and identify the total number of forms submitted in the blank below.

☑ A total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public, which is to update (and by the USPTO to process) the file of a patent or reexamination proceeding. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: MYPORT, INC.

Application No./Patent No.: 10237067 Filed/Issue Date: 3/19/2019

Titled: APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL TAGS

MYPORT, INC., a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Michael F. Malone To: MyPort Technologies, Inc.

   The document was recorded in the United States Patent and Trademark Office at
   Reel 044493, Frame 0702, or for which a copy thereof is attached.

2. From: MyPort Technologies, Inc. To: MyPort IP, Inc.

   The document was recorded in the United States Patent and Trademark Office at
   Reel 045082, Frame 0529, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: MyPort IP, Inc. To: MyPort, Inc.

The document was recorded in the United States Patent and Trademark Office at
Reel 059507, Frame 0960, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Signature	1-23-20 Date
Michael F. Malone Printed or Typed Name	CEO Title or Registration Number

AO 120 (Rev. 08/10)

TO:	**Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following ☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-114	4/15/2022	Eastern District of Texas
PLAINTIFF MYPORT, INC.		DEFENDANT SAMSUNG ELECTRONICS CO., LTD and SAMSUNG ELECTRONICS AMERICA, INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 9,832,017	11/28/2017	MyPort, Inc.
2 10,237,067	3/19/2019	MyPort, Inc.
3 10,721,066	7/21/2020	MyPort, Inc.
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

American LegalNet, Inc.
www.FormsWorkFlow.com

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/824,087	03/19/2019	10237067	MPOR60-33823	5197

25883 7590 02/27/2019

MUNCK WILSON MANDALA L.L.P
P.O. Drawer 800889
DALLAS, TX 75380

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Michael F. Malone, McKinney, TX;
MYPORT TECHNOLOGIES, INC., McKinney, TX;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

IR103 (Rev. 10/09)

Attorney Docket No. MPOR60-33823

SUPPLEMENTAL DECLARATION

Title of Invention: APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL TAGS, STORAGE AND SEARCH RETRIEVAL

This declaration is directed to (check one):

- ☐ the attached application;
- ☐ the application identified by the attorney docket no. and title of invention given above;
- ☒ United States Application or PCT International Application No. 15/824,087, filed November 28, 2017.

As a below-named inventor, I hereby declare that:

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I have reviewed and understand the contents of the above-identified specification, including the claims as originally filed and as amended in the amendments filed on September 10, 2018 and November 2, 2018; and

I acknowledge my duty to disclose information of which I am aware which is material to the patentability of this application in accordance with 37 C.F.R. § 1.56.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. § 1001 by fine or imprisonment of not more than five (5) years, or both.

Signature:  1/29/19

Inventor: Michael F. MALONE DATE

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

25883 7590 11/14/2018
MUNCK WILSON MANDALA L.L.P
P.O. Drawer 800889
DALLAS, TX 75380

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/824,087	11/28/2017	Michael F. Malone	MPOR60-33823	5197

TITLE OF INVENTION: APPARATUS FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAG(S)/ CONTEXTUAL TAG(S), STORAGE AND SEARCH/RETRIEVAL

APPLN. TYPE	SMALL ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	02/14/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHERALI, ISHRAT I	2667	382-100000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Gregory M. Howison
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: MyPort Technologies, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): McKinney, Texas

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☒ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☐ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 500208

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Gregory M. Howison, Reg. #30646/ Date January 29, 2019

Typed or printed name Gregory M. Howison Registration No. 30646

PTOL-85 Part B (08-18) Approved for use through 01/31/2020 OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Electronic Patent Application Fee Transmittal

Application Number:	15824087
Filing Date:	28-Nov-2017
Title of Invention:	APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/ CONTEXTUAL TAGS, STORAGE AND SEARCH RETRIEVAL
First Named Inventor/Applicant Name:	Michael F. Malone
Filer:	Gregory Michael Howison/Anna Nguyen
Attorney Docket Number:	MPOR60-33823

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
UTILITY APPL ISSUE FEE	1501	1	1000	1000
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1000**

Electronic Acknowledgement Receipt	
EFS ID:	34992764
Application Number:	15824087
International Application Number:	
Confirmation Number:	5197
Title of Invention:	APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/ CONTEXTUAL TAGS, STORAGE AND SEARCH RETRIEVAL
First Named Inventor/Applicant Name:	Michael F. Malone
Customer Number:	25883
Filer:	Gregory Michael Howison
Filer Authorized By:	
Attorney Docket Number:	MPOR60-33823
Receipt Date:	29-JAN-2019
Filing Date:	28-NOV-2017
Time Stamp:	14:18:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1000
RAM confirmation Number	013019INTEFSW14190100
Deposit Account	500208
Authorized User	Gregory Howison
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	MPO33823SuppDecEXE.pdf	363879 aede00ecfba7b8edbf85cd29dfb784f3fd8aabd9	no	1
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	MPO33823IssueFeeTransmittal.pdf	991704 9e599dd272d3e960e8fc64944df5e825e9b65e33	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	32219 3a929815d9821891b4728733be00c261ee50388e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1387802		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/824,087	11/28/2017	2667	1600	MPOR60-33823	20	2

CONFIRMATION NO. 5197

CORRECTED FILING RECEIPT

25883
MUNCK WILSON MANDALA L.L.P
P.O. Drawer 800889
DALLAS, TX 75380

OC000000105050050

Date Mailed: 01/14/2019

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Michael F. Malone, McKinney, TX;

Applicant(s)

MYPORT TECHNOLOGIES, INC., McKinney, TX;

Power of Attorney: The patent practitioners associated with Customer Number 25883

Domestic Priority data as claimed by applicant

This application is a CON of 15/272,013 09/21/2016 PAT 9832017
which is a CON of 14/660,166 03/17/2015 ABN
which is a CON of 13/965,625 08/13/2013 PAT 8983119
which is a CON of 13/417,229 03/10/2012 PAT 8509477
which is a CON of 12/857,358 08/16/2010 PAT 8135169
which is a CON of 11/621,062 01/08/2007 PAT 7778438
which is a CIP of 11/325,373 01/04/2006 PAT 7184573
and claims benefit of 60/757,075 01/06/2006
and said 11/325,373 01/04/2006
is a CON of 10/674,910 09/29/2003 PAT 6996251
which claims benefit of 60/414,449 09/30/2002

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 12/08/2017

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/824,087**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No

Title

APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL TAGS, STORAGE AND SEARCH RETRIEVAL

Preliminary Class

382

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor

community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/824,087	11/28/2017	2667	1600	MPOR60-33823	20	2

CONFIRMATION NO. 5197

CORRECTED FILING RECEIPT

25883
MUNCK WILSON MANDALA L.L.P
P.O. Drawer 800889
DALLAS, TX 75380

OC000000105049904

Date Mailed: 01/14/2019

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Michael F. Malone, McKinney, TX;

Applicant(s)

MYPORT TECHNOLOGIES, INC., McKinney, TX;

Power of Attorney: The patent practitioners associated with Customer Number 25883

Domestic Priority data as claimed by applicant

This application is a CON of 15/272,013 09/21/2016 PAT 9832017
which is a CON of 14/660,166 03/17/2015 ABN
which is a CON of 13/965,625 08/13/2013 PAT 8983119
which is a CON of 13/417,229 03/10/2012 PAT 8509477
which is a CON of 12/857,358 08/16/2010 PAT 8135169
which is a CON of 11/621,062 01/08/2007 PAT 7778438
which is a CIP of 11/325,373 01/04/2006 PAT 7184573
and claims benefit of 60/757,075 01/06/2006
and said 11/325,373 01/04/2006
is a CON of 10/674,910 09/29/2003 PAT 6996251
which claims benefit of 60/414,449 09/30/2002

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 12/08/2017

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/824,087**

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No

Title

APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL, STORAGE AND SEARCH RETRIEVAL

Preliminary Class

382

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor

community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

25883 7590 11/14/2018

MUNCK WILSON MANDALA L.L.P
P.O. Drawer 800889
DALLAS, TX 75380

EXAMINER	
SHERALI, ISHRAT I	
ART UNIT	PAPER NUMBER
2667	

DATE MAILED: 11/14/2018

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/824,087	11/28/2017	Michael F. Malone	MPOR60-33823	5197

TITLE OF INVENTION: APPARATUS FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAG(S)/ CONTEXTUAL TAG(S), STORAGE AND SEARCH RETRIEVAL

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	02/14/2019

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PTOL-85 (Rev. 02/11)

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

25883 7590 11/14/2018
MUNCK WILSON MANDALA L.L.P
P.O. Drawer 800889
DALLAS, TX 75380

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/824,087	11/28/2017	Michael F. Malone	MPOR60-33823	5197

TITLE OF INVENTION: APPARATUS FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAG(S)/ CONTEXTUAL TAG(S), STORAGE AND SEARCH/RETRIEVAL

APPLN. TYPE	SMALL ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	02/14/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHERALI, ISHRAT I	2667	382-100000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1_____
2_____
3_____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required) ❑Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/824,087	11/28/2017	Michael F. Malone	MPOR60-33823	5197

25883 7590 11/14/2018

MUNCK WILSON MANDALA L.L.P
P.O. Drawer 800889
DALLAS, TX 75380

EXAMINER	
SHERALI, ISHRAT I	
ART UNIT	PAPER NUMBER
2667	

DATE MAILED: 11/14/2018

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 15/824,087	Applicant(s) Malone, Michael F.	
	Examiner ISHRAT I SHERALI	Art Unit 2667	AIA Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 11/2/2018 and 9/10/2018.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are See Continuation Sheet . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file areply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/ISHRAT I SHERALI/
Primary Examiner, Art Unit 2667

Continuation of 3. The allowed claim(s) is/are: 21-37 (renumbered claims as 1-17)

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/824,087	Malone, Michael F.
	Examiner	**Art Unit**
	ISHRAT I SHERALI	2667

CPC						
Symbol					**Type**	**Version**
H04L	/	9	/	14	F	2013-01-01
G06F	/	17	/	30038	I	2013-01-01
G06F	/	17	/	30244	I	2013-01-01
G06F	/	17	/	30749	I	2013-01-01
H04L	/	9	/	3263	I	2013-01-01
H04L	/	9	/	3271	I	2013-01-01
H04L	/	9	/	3297	I	2013-01-01
H04N	/	5	/	76	I	2013-01-01
G06F	/	17	/	30268	I	2013-01-01
G06F	/	17	/	3028	I	2013-01-01
H04N	/	5	/	44	I	2013-01-01
H04N	/	21	/	25816	I	2013-01-01
H04N	/	21	/	25875	I	2013-01-01
H04N	/	21	/	26603	I	2013-01-01
H04N	/	21	/	26613	I	2013-01-01
H04N	/	21	/	2747	I	2013-01-01
H04N	/	21	/	4108	I	2013-01-01
H04N	/	21	/	6582	I	2013-01-01
H04N	/	21	/	835	I	2013-01-01
H04N	/	21	/	84	I	2013-01-01
H04L	/	2209	/	60	A	2013-01-01
H04L	/	2209	/	80	A	2013-01-01
H04N	/	5	/	77	A	2013-01-01
H04N	/	5	/	9201	A	2013-01-01

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	17	
/ISHRAT I SHERALI/ Primary Examiner, Art Unit 2667	05 November 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20181105

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/824,087	Malone, Michael F.
	Examiner	**Art Unit**
	ISHRAT I SHERALI	2667

INTERNATIONAL CLASSIFICATION					
CLAIMED					
H04L	/	9	/	14	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
382	100

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					
382	305					

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 17	
/ISHRAT I SHERALI/ Primary Examiner, Art Unit 2667 (Primary Examiner) (Date) 05 November 2018	O.G. Print Claim(s) 1	O.G. Print Figure 1

U.S. Patent and Trademark Office Part of Paper No.: 20181105

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/824,087	Malone, Michael F.
	Examiner	**Art Unit**
	ISHRAT I SHERALI	2667

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		10		19	8	28	17	37						
	2		11		20	9	29								
	3		12	1	21	10	30								
	4		13	2	22	11	31								
	5		14	3	23	12	32								
	6		15	4	24	13	33								
	7		16	5	25	14	34								
	8		17	6	26	15	35								
	9		18	7	27	16	36								

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	17	
/ISHRAT I SHERALI/ Primary Examiner, Art Unit 2667	05 November 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20181105

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/824,087	Malone, Michael F.
	Examiner	Art Unit
	ISHRAT I SHERALI	2667

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	03/01/2018	11/05/2018							
	1	✓	-							
	2	✓	-							
	3	✓	-							
	4	✓	-							
	5	✓	-							
	6	✓	-							
	7	✓	-							
	8	✓	-							
	9	✓	-							
	10	✓	-							
	11	✓	-							
	12	✓	-							
	13	✓	-							
	14	✓	-							
	15	✓	-							
	16	✓	-							
	17	✓	-							
	18	✓	-							
	19	✓	-							
	20	✓	-							
1	21		=							
2	22		=							
3	23		=							
4	24		=							
5	25		=							
6	26		=							
7	27		=							
8	28		=							
9	29		=							
10	30		=							
11	31		=							
12	32		=							
13	33		=							
14	34		=							
15	35		=							
16	36		=							
17	37		=							

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/824,087	Malone, Michael F.
	Examiner	**Art Unit**
	ISHRAT I SHERALI	2667

CPC - Searched*		
Symbol	**Date**	**Examiner**

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
382	100, 305	11/05/2018	IS

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**
SEARCH EAST TEXT LIMITED CPC/USPC, INVENTOR/ASSINGEE, GOOGLE	11/05/2018	IS
SEARCH EAST TEXT LIMITED FOLLOWING CPC CLASS/SUBCLASS: G06F 17/30038, 30749, 30268, 30244, H04L 9/14, H04N 5/76, 44, H04N 21/25816, 25875, 26603, 26613	11/05/2018	IS

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
	SEARCH INTERFERENCE TEXT LIMITED CPC/ USPC	11/05/2018	IS

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8424227		2013-04-23	HARRINGTON, JOHN	
	2	8099772		2012-01-17	TAKADA ET AL.	
	3	6968453		2005-11-22	DOYLE ET AL.	
	4	6996251		2006-02-07	MALONE ET AL.	
	5	4742369		1988-05-03	ISHII ET AL.	
	6	5031122		1991-07-09	WITTY	
	7	5276472		1994-01-04	BELL ET AL.	
	8	5546145		1996-08-13	BERNARDI ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	9	5786851		1998-07-28	KONDO ET AL.	
	10	5940121		1999-08-17	MCINTYRE ET AL.	
	11	5995936		1999-11-30	BRAIS ET AL.	
	12	6031526		2000-02-29	SHIPP	
	13	7617542		2009-11-10	VATAJA	
	14	6104430		2000-08-15	FUKUOKA	
	15	6683649		2004-01-27	ANDERSON	
	16	7053938		2006-05-30	SHERRY	
	17	7907199		2011-03-15	SEKI ET AL.	
	18	7831598		2010-11-09	KO	
	19	7324943		2008-01-29	RIGAZIO ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	20	7961218		2011-06-14	SEKI ET AL.	
	21	6115137		2000-09-05	OZAWA ET AL	
	22	6111605		2000-08-09	SUZUKI	
	23	7319484		2008-01-15	YOSHIDA ET AL	
	24	6222985		2001-04-24	MIYAKE	
	25	6741864		2004-05-25	WILCOCK, ET AL.	
	26	6636158		2003-10-21	BANDO, ET AL.	
	27	6525768		2003-02-25	OBRADOVICH	
	28	6720879		2004-04-03	EDWARDS	
	29	6507371		2003-01-14	HASHIMOTO, ET AL.	
	30	6498586		2002-12-24	PANKINAHO	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	31	6292633		2001-09-18	NAKAGAWA	
	32	6198989		2001-03-06	TANKHILEVICH, ET AL.	
	33	5768640		1998-06-16	TAKAHASHI, ET AL.	
	34	5642285		1997-06-24	WOO, ET AL.	
	35	6560660		2003-05-06	FLANAGIN	
	36	6526351		2003-02-25	WHITHAM	
	37	6160964		2000-12-12	IMOTO	
	38	6532298		2003-03-11	CAMBIER, ET AL.	
	39	6205249		2001-03-20	MOSKOWITZ	
	40	6185683		2001-02-06	GINTER, ET AL.	
	41	6714778		2004-03-30	NYKANEN, ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	42	6166729		2000-12-26	ACOSTA, EDWARD	
	43	6424968		2002-07-23	BROSTER, ET AL.	
	44	6065119		2000-05-16	SANDFORD, II, ET AL.	
	45	6462778		2002-10-08	ABRAM, ET AL.	
	46	6505160		2003-01-07	LEVY, ET AL.	
	47	6526215		2003-02-25	HIRAI, ET AL.	
	48	6606117		2003-08-12	WINDLE	
	49	2950971		1960-08-30	LEWIN	
	50	3439598		1969-04-22	WEITZNER, ET AL.	
	51	5602458		1997-02-11	DOWE	
	52	5692225		1997-11-25	BERNARDI, ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	53	6681029		2004-01-20	RHOADS	
	54	7010144		2006-03-07	DAVIS ET AL.	
	55	7043048		2006-05-09	ELLINGSON	
	56	0055422		1866-06-05	ROUSTAEI	
	57	4015240		1977-03-29	SWONGER ET AL.	
	58	4109237		1978-08-22	HILL	
	59	4528588		1985-07-09	LOFBERG	
	60	4620318		1986-10-28	HILL	
	61	4994831		1991-02-19	MARANDI	
	62	4995086		1991-02-19	LILLEY ET AL.	
	63	5103486		1992-04-07	GRIPPI	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	64	5767496		1998-06-16	SWARTZ ET AL.	
	65	5787183		1998-07-28	SCHROEDER	
	66	5799092		1998-08-25	KRISTOL ET AL.	
	67	5841886		1998-11-24	RHOADS	
	68	5857038		1999-01-05	OWADA ET AL.	
	69	5907149		1999-05-25	MARCKINI	
	70	5995630		1999-11-30	BORZA	
	71	6005936		1999-12-21	SCHIMIZU ET AL.	
	72	6064764		2000-05-16	BHASKARAN ET AL.	
	73	6148091		2000-11-24	DIMARIA	
	74	6185316		2001-02-06	BUFFAM	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	75	6208746		2001-03-27	MUSGRAVE	
	76	6243481		2001-06-05	TAO	
	77	6292092		2001-09-18	CHOW ET AL.	
	78	6301368		2001-10-09	BOLLE ET AL.	
	79	6321981		2001-11-27	RAY ET AL.	
	80	6366680		2002-04-02	BRUNK ET AL.	
	81	6377699		2002-04-23	MUSGRAVE ET AL.	
	82	6389151		2002-05-14	CARR ET AL.	
	83	6397334		2002-05-28	CHAINER ET AL.	
	84	6577336		2003-06-10	SAFAI	
	85	6687383		2004-02-03	KANEVSKY ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	86	7778440		2010-08-17	MALONE, MICHAEL F.	
	87	8068638		2011-11-29	MALONE, MICHAEL F.	
	88	7184573		2007-02-27	MALONE ET AL.	
	89	6023241		2000-02-08	CLAPPER	
	90	5913078		1999-06-15	KIMURA ET AL.	
	91	5732354		1998-03-24	MACDONALD	
	92	6212401		2001-04-03	ACKLEY	
	93	5825890		1998-10-20	ELGAMAL ET AL.	
	94	8135169		2012-03-13	MALONE, MICHAEL F.	
	95	6914695		2005-07-05	WALTERS ET AL.	
	96	5247300		1993-09-21	SOHN, SUNG W.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	97	7778438		2010-08-17	MALONE, MICHAEL F.	
	98	RE39526		2007-03-20	HULL ET AL.	
	99	52670425		1993-11-30	TSUCHIYA ET AL.	
	100	5515042		1996-05-07	NELSON	
	101	5712679		1998-01-27	COLES	
	102	5726660		1998-03-10	PURDY ET AL.	
	103	5806005		1998-09-08	HULL ET AL.	
	104	6181373		2001-01-30	COLES	
	105	6359837		2002-03-19	TSUKAMOTO	
	106	6571271		2003-05-27	SAVITZKY ET AL.	
	107	6831682		2004-12-14	SILVERBROOK ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	108	6833861		2004-12-21	MATSUMOTO ET AL.	
	109	7016899		2006-03-21	STERN ET AL.	
	110	7265779		2007-09-04	SATO ET AL.	
	111	6889324		2005-05-03	KANAI ET AL.	
	112	6853987		2005-02-08	COOK, DAVID P.	
	113	6269446		2001-07-31	SCHUMACHER ET AL.	
	114	6968366		2005-11-22	ZHANG ET AL.	
	115	7391960		2008-06-24	SHINOZAKI ET AL.	
	116	6990444		2006-01-24	HIND ET AL.	
	117	5737491		1998-04-07	ALLEN ET AL.	
	118	4115805		1978-09-19	MORTON	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	119	4334241		1982-06-08	KASHIOKA, ET AL.	
	120	4574319		1986-03-04	KONISHI	
	121	5335072		1994-08-02	TANAKA, ET AL.	
	122	5506644		1996-04-09	SUZUKI, ET AL.	
	123	5633678		1997-05-27	PARULSKI, ET AL.	
	124	6332193		2001-12-18	GLASS, ET AL.	
	125	6219560		2001-04-17	ERKKILA, MARKO	
	126	6014183		2000-01-11	HOANG	
	127	6115717		2000-09-05	MEHROTRA ET AL.	
	128	5819289		1998-10-06	SANFORD, II ET AL.	
	129	5657077		1997-08-12	DEANGELIS, ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	130	5682458		1997-10-28	FUNAZAKI	
	131	5692104		1997-11-25	CHOW, ET AL.	
	132	5706457		1998-01-06	DWYER, ET AL.	
	133	5796428		1998-08-18	MATSUMOTO, ET AL.	
	134	5828809		1998-10-27	CHANG, ET AL.	
	135	5835667		1998-11-10	WACTLAR, ET AL.	
	136	5872865		1999-02-16	NORMILE, ET AL.	
	137	5889578		1999-03-30	JAMZADEH	
	138	5893095		1999-04-06	JAIN, ET AL.	
	139	6282362		2001-08-28	MURPHY, ET AL.	
	140	5499294		1996-03-12	FRIEDMAN, GARY L.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	141	5815201		1998-09-29	HASHIMOTO ET AL.	
	142	4389109		1983-06-21	TANIGUCHI ET AL.	
	143	4270853		1981-06-02	HATADA ET AL.	
	144	4270854		1981-06-02	STEMME ET AL.	
	145	4344682		1982-08-17	HATTORI	
	146	4443077		1984-04-17	TANIKAWA	
	147	4613911		1986-09-23	OHTA	
	148	4642717		1987-02-10	MATSUDA ET AL.	
	149	4905029		1990-02-27	KELLEY	
	150	4951079		1990-08-21	HOSHINO ET AL.	
	151	4965626		1990-10-23	ROBISON ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	152	4977419		1990-12-11	WASH ET AL.	
	153	4983996		1991-01-08	KINOSHITA	
	154	5023635		1991-06-11	NEALON	
	155	5025283		1991-06-18	ROBINSON	
	156	5027149		1991-06-25	HOSHINO ET AL.	
	157	5070355		1991-12-03	INOUE ET AL.	
	158	5097278		1992-03-17	TAMAMURA ET AL.	
	159	5099262		1992-03-24	TANAKA ET AL.	
	160	5128700		1992-07-07	INOUE ET AL.	
	161	5142310		1992-08-25	TANIGUCHI ET AL.	
	162	5146249		1992-09-08	HODA ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	163	5160952		1992-11-03	IWASHITA ET AL.	
	164	5245372		1993-09-14	OASHIMA	
	165	5313235		1994-05-17	INOUE ET AL.	
	166	5426745		1995-06-20	BAJI ET AL.	
	167	6952164		2005-10-04	JUNQUA	
	168	6959868		2005-11-01	TSIKOS ET AL.	
	169	6965324		2005-11-15	SUGGS, SR.	
	170	6956671		2005-10-18	MONTY ET AL.	
	171	6895126		2005-05-17	DI BERNARDO ET AL.	
	172	6856344		2005-02-15	FRANZ	
	173	6750902		2004-06-15	STEINBERG ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	174	6747692		2004-06-08	PATEL ET AL.	
	175	6670984		2003-12-30	TANAKA ET AL.	
	176	6628325		2003-12-30	STEINBERG ET AL.	
	177	6535298		2003-03-18	WINTER ET AL	
	178	6411328		2002-06-25	FRANKE ET AL.	
	179	7095871		2006-08-22	JONES ET AL.	
	180	5841978		1998-11-24	RHOADS	
	181	5410598		1995-04-25	SHEAR	
	182	5493677		1996-02-20	BALOGH ET AL.	
	183	5502576		1996-03-26	RAMSAY ET AL.	
	184	5519778		1996-05-21	LEIGHTON ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	185	5530759		1996-06-25	BRAUDAWAY ET AL.	
	186	5568570		1996-10-22	RABBANI	
	187	5581800		1996-12-03	FARDEAU ET AL.	
	188	5617119		1997-04-01	BRIGGS ET AL.	
	189	5629980		1997-05-13	STEFIK	
	190	5646990		1997-07-08	LI	
	191	5646997		1997-07-08	BARTSON	
	192	5740244		1998-04-14	INDECK ET AL.	
	193	5765152		1998-06-09	ERICKSON	
	194	5822432		1998-10-13	MOSKOWITZ ET AL.	
	195	5845281		1998-12-01	BENSON	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	196	5862260		1999-01-19	RHOADS	
	197	5892900		1999-04-06	GINTER ET AL.	
	198	5923327		1999-07-13	SMITH ET AL.	
	199	5943422		1999-08-24	VAN WIE ET AL.	
	200	5978773		1999-11-02	HUDETZ ET AL.	
	201	5991876		1999-11-23	JOHNSON ET AL.	
	202	6014569		2000-01-11	BOTTUM	
	203	6122403		2000-09-19	RHOADS	
	204	6141753		2000-10-31	ZHAO ET AL.	
	205	6233684		2001-05-15	STEFIK ET AL.	
	206	6243480		2001-06-05	ZHAO ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	207	6282654		2001-08-28	IKEDA ET AL.	
	208	6300880		2001-10-09	SITNIK	
	209	6334187		2001-12-25	KADONO	
	210	6363043		2002-03-26	KONDO	
	211	6389538		2002-05-14	GRUSE ET AL.	
	212	6421450		2002-07-16	NAKANO	
	213	6437933		2002-08-20	SUGIYAMA ET AL.	
	214	6449367		2002-09-10	VAN WIE ET AL.	
	215	6469969		2002-10-22	CARSON ET AL.	
	216	6491217		2002-12-10	CATAN	
	217	6560339		2003-05-06	IWAMURA	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	218	6591365		2003-07-08	COOKSON	
	219	6611607		2003-08-26	DAVIS ET AL	
	220	6636249		2003-10-21	REKIMOTO	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040114042		2004-06-17	PAOLINI, MICHAEL A., ET AL.	
	2	20030177094		2003-09-18	NEEDHAM, BRADFORD H., ET AL.	
	3	20040103283		2004-05-27	HOMAK, ZOLTAN	
	4	20040101138		2004-05-27	REVITAL, DAN, ET AL.	
	5	20040091111		2004-05-13	LEVY, KENNETH L., ET AL.	
	6	20040073568		2004-04-15	YONAHA, MAKOTO	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	7	20040073557		2004-04-15	PICCIONELLI, GREGORY A., ET AL.	
	8	20040068371		2004-04-08	ESTEP, RANDALL S.	
	9	20040053637		2004-03-18	IIDA, TAKAYUKI	
	10	20040049734		2004-03-11	SIMSKE, STEVEN J.	
	11	20040044911		2004-03-04	TAKADA, MASAYUKI	
	12	20040039930		2004-02-26	OHMORI, MOTOJI, ET AL.	
	13	20040032499		2004-02-19	SILVERBROOK, KIA, ET AL.	
	14	20040023686		2004-02-05	KING, JOHN J., ET AL.	
	15	20040005078		2004-01-08	TILLOTSON, SCOTT ANDREW	
	16	20040022444		2004-02-05	RHOADS, GEOFFREY B.	
	17	20020073056		2002-06-13	BROSTER, IAN, ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	18	20010012062		2001-08-09	ANDERSON	
	19	20020191087		2002-12-19	HASHIMOTO, ET AL.	
	20	20030048921		2003-03-13	CAHALL, NATHAN D.	
	21	20020194480		2002-12-19	NAGAO, KATASHI	
	22	20030011684		2003-01-16	NARAYANASWAMI ET AL.	
	23	20030032033		2003-02-13	ANGLIN ET AL.	
	24	20050043018		2005-02-24	KAWAMOTO, YOJI	
	25	20060018506		2006-01-26	RODRIGUEZ ET AL.	
	26	20070055689		2007-03-08	RHOADS ET AL.	
	27	20010007130		2001-07-05	TAKARAGI	
	28	20010011680		2001-08-09	SOLTESZ ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	29	20010025342		2001-09-27	UCHIDA	
	30	20010034835		2001-10-25	SMITH	
	31	20020010684		2002-01-24	MOSKOWITZ	
	32	20020061120		2002-05-23	CARR ET AL.	
	33	20020072935		2002-06-13	ROWSE ET AL.	
	34	20010015759		2001-08-23	SQUIBBS	
	35	20010012066		2001-08-09	PARULSKI ET AL.	
	36	20010018349		2001-08-30	KINNUNEN ET AL.	
	37	20020046188		2002-04-18	BURGES ET AL.	
	38	20040197013		2004-10-07	KAMEI	
	39	20050134703		2005-06-23	MITTAL	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	40	20070250526		2007-10-25	HANNA	
	41	20070098172		2007-05-03	LEVY ET AL.	
	42	20030187950		2003-10-02	RISING III	
	43	20050231752		2005-10-20	SAINIO, KARI	
	44	20050219359		2005-10-06	TRELA, RICHARD STEVEN	
	45	20050216949		2005-09-29	CANDELORA ET AL.	
	46	20050216580		2005-09-29	RAJI ET AL.	
	47	20050185049		2005-08-25	IWAI ET AL.	
	48	20050143136		2005-06-30	LEV ET AL.	
	49	20050094000		2005-05-05	SON ET AL.	
	50	20050091311		2005-04-28	LUND ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	51	20050041035		2005-02-24	NAGATOMO ET AL.	
	52	20050024493		2005-02-03	NAM, KI Y.	
	53	20040257431		2004-12-23	GIRISH ET AL.	
	54	20040203386		2004-10-14	TISCHER ET AL.	
	55	20040183915		2004-09-23	GOTOHDA, ET AL.	
	56	20040148518		2004-07-29	GRUNDBACK ET AL.	
	57	20040109199		2004-06-10	TSUBAKI, HISAYOSHI	
	58	20040085203		2004-05-06	JUNQUA, JEAN-CLAUDE	
	59	20040070670		2004-04-15	FOSTER, WARD S.	
	60	20010021144		2001-09-13	OSHIMA ET AL.	
	61	20010021978		2001-09-13	OKAYASU ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	62	20010044824		2001-11-22	HUNTER ET AL.	
	63	20020001395		2002-01-03	DAVIS ET AL.	
	64	20020015042		2002-02-07	ROBOTHAM ET AL.	
	65	20020030907		2002-03-14	IKEDA ET AL.	
	66	20020031240		2002-03-14	LEVY ET AL.	
	67	20020032502		2002-03-14	RUSSELL, J. CHRIS	
	68	20020033844		2002-03-21	LEVY ET AL.	
	69	20020051577		2002-05-02	KINJO, NAOTO	
	70	20020059162		2002-05-16	SHINODA ET AL.	
	71	20020062382		2002-05-23	RHOADS ET AL.	
	72	20020075298		2002-06-20	SCHENA ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	73	20020080271		2002-06-27	EVELEENS ET AL.	
	74	20020080396		2002-06-27	SILVERBROOK ET AL.	
	75	20020080964		2002-06-27	STONE ET AL.	
	76	20020083123		2002-06-27	FREEDMAN ET AL.	
	77	20020102966		2002-08-01	LEV ET AL.	
	78	20020146148		2002-10-10	LEVY, KENNETH L.	
	79	20020152388		2002-10-17	LINNARTZ ET AL.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	0905966	EP		1999-03-31	CANON KABUSHIKI KAISHA		
	2	0152178	WO		2001-07-19	DIGIMARC CORPORATION		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	3	9901859	WO		1999-01-14	IMIGE INCORPORATED		
	4	0167707	WO		2001-09-13	SCALE EIGHT, INCORPORATED		
	5	1204277	EP		2002-05-08	TEKTRONIX, INC.		
	6	9743736	WO		1997-11-20	DIGIMARC CORPORATION		
	7	9626494	WO		1996-08-29	THE REGENTS OF THE UNIVERSITY OF CALIFORNIA		
	8	9936876	WO		1999-07-22	DIGIMARC CORPORATION		
	9	0115021	WO		2001-03-01	DIGITAL CONVERGENCE.:COM INC.		
	10	0161508	WO		2001-08-23	DIGIMARC CORPORATION		
	11	0173586	WO		2001-10-04	DIGITAL: CONVERGENCE CORPORATION		
	12	0175629	WO		2001-10-11	NEOMEDIA TECHNOLOGIES, INC.		
	13	0197128	WO		2001-12-20	MARKANY INC.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	14	0211446	WO		2002-02-07	KONINKLIJKE PHILIPS ELECTRONICS, N.V.		
	15	9827510	WO		1998-06-25	THE REGENTS OF THE UNIVERSITY OF CALIFORNIA		
	16	0036605	WO		2000-06-22	KENT RIDGE DIGITAL LABS		
	17	0070585	WO		2000-11-23	DIGIMARC CORPORATION		
	18	9603286	WO		1996-02-08	INTERNATIONAL DATA MATRIX, INC.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,265; dated June 6, 2014; Examiner Angela M. Lie; 1085 pages 6 Jun 2014	
	2	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,255; dated May 27, 2014; Examiner Scott Louis Weaver; 906 pages 27 May 2014	
	3	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,265; dated February 16, 2015; Examiner Angela M. Lie; 187 pages 16 Feb 2015	
	4	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,255; dated March 2, 2015; Examiner Angela M. Lie; 177 pages 2 Mar 2015	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	5	H. KRAWCZYK, RFC 2104 (RFC2104) RFC 2104 - HMAC: Keyed-Hashing for Message Authentication https://www.faqs.org/rfcs/rfc2104.htm, February 1997.	
	6	G. Friedman, "The Trustworthy Digital Camera: Restoring Credibility To The Photographic Image," IEEE Transactions on Consumer Electronics, pages 905-910, Vol. 39, No. 4, November 1993.	
	7	FRANKS, et al., "HTTP Authentication: Basic and Digest Access Authentication," The Internet Society, June 1999.	
	8	FRANKS, et al., "An Extension to HTTP: Digest Access Authentication," The Internet Society, January 1997.	
	9	Supplemental First Amended Complaint, MyPort IP, Inc. v. HTC Corporation, Civil Action No. 6:11-cv-00246 (E.D. Tex. Filed March 8, 2012) ("MyPort Complaint"), 12 pages. 8 Mar 2012	
	10	Digital Still Camera Image File Format Standard (Exchangeable image file format for Digital Still Cameras: Exif), Version 2.1, published June 12, 1998 by the Japan Electronic Industry Development Association (JEIDA) ("Exif 2.1 Specification"), 173 pages.	
	11	TIFF Specification Revision 6.0, Aldus Developers Desk, Aldus Corporation, June 3, 1992.	
	12	James Bao-Yen Tsui, Fundamental of Global Positioning System Receivers: A Software Approach, pages 1-6, 73-108, 1983-217 (John Wiley & Sons, Inc. 2000).	
	13	PPP Encryption Control Protocol, Internet Engineering Task Force (IETF), published June 1996.	
	14	Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography (CRC Press 1996).	
	15	MyPort IP, Inc.'s Disclosure Pursuant to Patent Rule 3-1, MyPort IP, Inc. v. HTC Corporation, Civil Action No. 6:11-cv-00246 (E.D. Tex. Filed May 13, 2011).	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	16	STANSELL, Jr., "Civil GPS from a Future Perspective," Proceedings of the IEEE, October 1983, vol. 71, No. 10; pgs. 1187-1192. 1 Oct 1983	
	17	DALE, DIANA & ROG, RON, The Need For a Meta-Tag Standard for Audio and Visual Materials, Proc. Int. Conf. on Dublin Core and Metadata for e-Communities 2002: 205-206. 1 Jan 2002	
	18	KOSOVIC, DOUGLAS; SCHROETER, RONALD; and HUNTER, JANE, Collaborative Video Annotation, Indexing and Discussion over high-bandwidth networks, DSTC Technical Report TR247, 2002, DSTC Pty Ltd., St Lucia, Qld, Australia. 1 Jan 2002	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISHRAT I SHERALI/	Date Considered	11/05/2018

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith D. Harden, Reg. # 74472/	Date (YYYY-MM-DD)	2018-04-23
Name/Print	Keith D. Harden	Registration Number	74472

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5267042		1993-11-30	TSUCHIYA ET AL.	
	2	6947571		2005-09-20	RHOADS ET AL.	
	3	6807534		2004-10-19	ERICKSON	
	4	6788800		2004-09-07	CARR ET AL	
	5	6786397		2004-09-07	SILVERBROOK ET AL	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISHRAT I SHERALI/	Date Considered	11/05/2018

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith D. Harden, Reg. # 74472/	Date (YYYY-MM-DD)	2018-04-23
Name/Print	Keith D. Harden	Registration Number	74472

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8424227		2013-04-23	HARRINGTON, JOHN	
	2	8099772		2012-01-17	TAKADA ET AL.	
	3	6968453		2005-11-22	DOYLE ET AL.	
	4	6996251		2006-02-07	MALONE ET AL.	
	5	4742369		1988-05-03	ISHII ET AL.	
	6	5031122		1991-07-09	WITTY	
	7	5276472		1994-01-04	BELL ET AL.	
	8	5546145		1996-08-13	BERNARDI ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	9	5786851		1998-07-28	KONDO ET AL.	
	10	5940121		1999-08-17	MCINTYRE ET AL.	
	11	5995936		1999-11-30	BRAIS ET AL.	
	12	6031526		2000-02-29	SHIPP	
	13	7617542		2009-11-10	VATAJA	
	14	6104430		2000-08-15	FUKUOKA	
	15	6683649		2004-01-27	ANDERSON	
	16	7053938		2006-05-30	SHERRY	
	17	7907199		2011-03-15	SEKI ET AL.	
	18	7831598		2010-11-09	KO	
	19	7324943		2008-01-29	RIGAZIO ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	20	7961218		2011-06-14	SEKI ET AL.	
	21	6115137		2000-09-05	OZAWA ET AL	
	22	6111605		2000-08-09	SUZUKI	
	23	7319484		2008-01-15	YOSHIDA ET AL	
	24	6222985		2001-04-24	MIYAKE	
	25	6741864		2004-05-25	WILCOCK, ET AL.	
	26	6636158		2003-10-21	BANDO, ET AL.	
	27	6525768		2003-02-25	OBRADOVICH	
	28	6720879		2004-04-03	EDWARDS	
	29	6507371		2003-01-14	HASHIMOTO, ET AL.	
	30	6498586		2002-12-24	PANKINAHO	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	31	6292633		2001-09-18	NAKAGAWA	
	32	6198989		2001-03-06	TANKHILEVICH, ET AL.	
	33	5768640		1998-06-16	TAKAHASHI, ET AL.	
	34	5642285		1997-06-24	WOO, ET AL.	
	35	6560660		2003-05-06	FLANAGIN	
	36	6526351		2003-02-25	WHITHAM	
	37	6160964		2000-12-12	IMOTO	
	38	6532298		2003-03-11	CAMBIER, ET AL.	
	39	6205249		2001-03-20	MOSKOWITZ	
	40	6185683		2001-02-06	GINTER, ET AL.	
	41	6714778		2004-03-30	NYKANEN, ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	42	6166729		2000-12-26	ACOSTA, EDWARD	
	43	6424968		2002-07-23	BROSTER, ET AL.	
	44	6065119		2000-05-16	SANDFORD, II, ET AL.	
	45	6462778		2002-10-08	ABRAM, ET AL.	
	46	6505160		2003-01-07	LEVY, ET AL.	
	47	6526215		2003-02-25	HIRAI, ET AL.	
	48	6606117		2003-08-12	WINDLE	
	49	2950971		1960-08-30	LEWIN	
	50	3439598		1969-04-22	WEITZNER, ET AL.	
	51	5602458		1997-02-11	DOWE	
	52	5692225		1997-11-25	BERNARDI, ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	53	6681029		2004-01-20	RHOADS	
	54	7010144		2006-03-07	DAVIS ET AL.	
	55	7043048		2006-05-09	ELLINGSON	
	56	0055422		1866-06-05	ROUSTAEI	
	57	4015240		1977-03-29	SWONGER ET AL.	
	58	4109237		1978-08-22	HILL	
	59	4528588		1985-07-09	LOFBERG	
	60	4620318		1986-10-28	HILL	
	61	4994831		1991-02-19	MARANDI	
	62	4995086		1991-02-19	LILLEY ET AL.	
	63	5103486		1992-04-07	GRIPPI	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	64	5767496		1998-06-16	SWARTZ ET AL.	
	65	5787183		1998-07-28	SCHROEDER	
	66	5799092		1998-08-25	KRISTOL ET AL.	
	67	5841886		1998-11-24	RHOADS	
	68	5857038		1999-01-05	OWADA ET AL.	
	69	5907149		1999-05-25	MARCKINI	
	70	5995630		1999-11-30	BORZA	
	71	6005936		1999-12-21	SCHIMIZU ET AL.	
	72	6064764		2000-05-16	BHASKARAN ET AL.	
	73	6148091		2000-11-24	DIMARIA	
	74	6185316		2001-02-06	BUFFAM	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	75	6208746		2001-03-27	MUSGRAVE	
	76	6243481		2001-06-05	TAO	
	77	6292092		2001-09-18	CHOW ET AL.	
	78	6301368		2001-10-09	BOLLE ET AL.	
	79	6321981		2001-11-27	RAY ET AL.	
	80	6366680		2002-04-02	BRUNK ET AL.	
	81	6377699		2002-04-23	MUSGRAVE ET AL.	
	82	6389151		2002-05-14	CARR ET AL.	
	83	6397334		2002-05-28	CHAINER ET AL.	
	84	6577336		2003-06-10	SAFAI	
	85	6687383		2004-02-03	KANEVSKY ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	86	7778440		2010-08-17	MALONE, MICHAEL F.	
	87	8068638		2011-11-29	MALONE, MICHAEL F.	
	88	7184573		2007-02-27	MALONE ET AL.	
	89	6023241		2000-02-08	CLAPPER	
	90	5913078		1999-06-15	KIMURA ET AL.	
	91	5732354		1998-03-24	MACDONALD	
	92	6212401		2001-04-03	ACKLEY	
	93	5825890		1998-10-20	ELGAMAL ET AL.	
	94	8135169		2012-03-13	MALONE, MICHAEL F.	
	95	6914695		2005-07-05	WALTERS ET AL.	
	96	5247300		1993-09-21	SOHN, SUNG W.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	97	7778438		2010-08-17	MALONE, MICHAEL F.	
	98	RE39526		2007-03-20	HULL ET AL.	
	99	52670425		1993-11-30	TSUCHIYA ET AL.	
	100	5515042		1996-05-07	NELSON	
	101	5712679		1998-01-27	COLES	
	102	5726660		1998-03-10	PURDY ET AL.	
	103	5806005		1998-09-08	HULL ET AL.	
	104	6181373		2001-01-30	COLES	
	105	6359837		2002-03-19	TSUKAMOTO	
	106	6571271		2003-05-27	SAVITZKY ET AL.	
	107	6831682		2004-12-14	SILVERBROOK ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	108	6833861		2004-12-21	MATSUMOTO ET AL.	
	109	7016899		2006-03-21	STERN ET AL.	
	110	7265779		2007-09-04	SATO ET AL.	
	111	6889324		2005-05-03	KANAI ET AL.	
	112	6853987		2005-02-08	COOK, DAVID P.	
	113	6269446		2001-07-31	SCHUMACHER ET AL.	
	114	6968366		2005-11-22	ZHANG ET AL.	
	115	7391960		2008-06-24	SHINOZAKI ET AL.	
	116	6990444		2006-01-24	HIND ET AL.	
	117	5737491		1998-04-07	ALLEN ET AL.	
	118	4115805		1978-09-19	MORTON	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	119	4334241		1982-06-08	KASHIOKA, ET AL.	
	120	4574319		1986-03-04	KONISHI	
	121	5335072		1994-08-02	TANAKA, ET AL.	
	122	5506644		1996-04-09	SUZUKI, ET AL.	
	123	5633678		1997-05-27	PARULSKI, ET AL.	
	124	6332193		2001-12-18	GLASS, ET AL.	
	125	6219560		2001-04-17	ERKKILA, MARKO	
	126	6014183		2000-01-11	HOANG	
	127	6115717		2000-09-05	MEHROTRA ET AL.	
	128	5819289		1998-10-06	SANFORD, II ET AL.	
	129	5657077		1997-08-12	DEANGELIS, ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	130	5682458		1997-10-28	FUNAZAKI	
	131	5692104		1997-11-25	CHOW, ET AL.	
	132	5706457		1998-01-06	DWYER, ET AL.	
	133	5796428		1998-08-18	MATSUMOTO, ET AL.	
	134	5828809		1998-10-27	CHANG, ET AL.	
	135	5835667		1998-11-10	WACTLAR, ET AL.	
	136	5872865		1999-02-16	NORMILE, ET AL.	
	137	5889578		1999-03-30	JAMZADEH	
	138	5893095		1999-04-06	JAIN, ET AL.	
	139	6282362		2001-08-28	MURPHY, ET AL.	
	140	5499294		1996-03-12	FRIEDMAN, GARY L.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	141	5815201		1998-09-29	HASHIMOTO ET AL.	
	142	4389109		1983-06-21	TANIGUCHI ET AL.	
	143	4270853		1981-06-02	HATADA ET AL.	
	144	4270854		1981-06-02	STEMME ET AL.	
	145	4344682		1982-08-17	HATTORI	
	146	4443077		1984-04-17	TANIKAWA	
	147	4613911		1986-09-23	OHTA	
	148	4642717		1987-02-10	MATSUDA ET AL.	
	149	4905029		1990-02-27	KELLEY	
	150	4951079		1990-08-21	HOSHINO ET AL.	
	151	4965626		1990-10-23	ROBISON ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	152	4977419		1990-12-11	WASH ET AL.	
	153	4983996		1991-01-08	KINOSHITA	
	154	5023635		1991-06-11	NEALON	
	155	5025283		1991-06-18	ROBINSON	
	156	5027149		1991-06-25	HOSHINO ET AL.	
	157	5070355		1991-12-03	INOUE ET AL.	
	158	5097278		1992-03-17	TAMAMURA ET AL.	
	159	5099262		1992-03-24	TANAKA ET AL.	
	160	5128700		1992-07-07	INOUE ET AL.	
	161	5142310		1992-08-25	TANIGUCHI ET AL.	
	162	5146249		1992-09-08	HODA ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	163	5160952		1992-11-03	IWASHITA ET AL.	
	164	5245372		1993-09-14	OASHIMA	
	165	5313235		1994-05-17	INOUE ET AL.	
	166	5426745		1995-06-20	BAJI ET AL.	
	167	6952164		2005-10-04	JUNQUA	
	168	6959868		2005-11-01	TSIKOS ET AL.	
	169	6965324		2005-11-15	SUGGS, SR.	
	170	6956671		2005-10-18	MONTY ET AL.	
	171	6895126		2005-05-17	DI BERNARDO ET AL.	
	172	6856344		2005-02-15	FRANZ	
	173	6750902		2004-06-15	STEINBERG ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	174	6747692		2004-06-08	PATEL ET AL.	
	175	6670984		2003-12-30	TANAKA ET AL.	
	176	6628325		2003-12-30	STEINBERG ET AL.	
	177	6535298		2003-03-18	WINTER ET AL	
	178	6411328		2002-06-25	FRANKE ET AL.	
	179	7095871		2006-08-22	JONES ET AL.	
	180	5841978		1998-11-24	RHOADS	
	181	5410598		1995-04-25	SHEAR	
	182	5493677		1996-02-20	BALOGH ET AL.	
	183	5502576		1996-03-26	RAMSAY ET AL.	
	184	5519778		1996-05-21	LEIGHTON ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	185	5530759		1996-06-25	BRAUDAWAY ET AL.	
	186	5568570		1996-10-22	RABBANI	
	187	5581800		1996-12-03	FARDEAU ET AL.	
	188	5617119		1997-04-01	BRIGGS ET AL.	
	189	5629980		1997-05-13	STEFIK	
	190	5646990		1997-07-08	LI	
	191	5646997		1997-07-08	BARTSON	
	192	5740244		1998-04-14	INDECK ET AL.	
	193	5765152		1998-06-09	ERICKSON	
	194	5822432		1998-10-13	MOSKOWITZ ET AL.	
	195	5845281		1998-12-01	BENSON	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	196	5862260		1999-01-19	RHOADS	
	197	5892900		1999-04-06	GINTER ET AL.	
	198	5923327		1999-07-13	SMITH ET AL.	
	199	5943422		1999-08-24	VAN WIE ET AL.	
	200	5978773		1999-11-02	HUDETZ ET AL.	
	201	5991876		1999-11-23	JOHNSON ET AL.	
	202	6014569		2000-01-11	BOTTUM	
	203	6122403		2000-09-19	RHOADS	
	204	6141753		2000-10-31	ZHAO ET AL.	
	205	6233684		2001-05-15	STEFIK ET AL.	
	206	6243480		2001-06-05	ZHAO ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	207	6282654		2001-08-28	IKEDA ET AL.	
	208	6300880		2001-10-09	SITNIK	
	209	6334187		2001-12-25	KADONO	
	210	6363043		2002-03-26	KONDO	
	211	6389538		2002-05-14	GRUSE ET AL.	
	212	6421450		2002-07-16	NAKANO	
	213	6437933		2002-08-20	SUGIYAMA ET AL.	
	214	6449367		2002-09-10	VAN WIE ET AL.	
	215	6469969		2002-10-22	CARSON ET AL.	
	216	6491217		2002-12-10	CATAN	
	217	6560339		2003-05-06	IWAMURA	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	218	6591365		2003-07-08	COOKSON	
	219	6611607		2003-08-26	DAVIS ET AL	
	220	6636249		2003-10-21	REKIMOTO	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040114042		2004-06-17	PAOLINI, MICHAEL A., ET AL.	
	2	20030177094		2003-09-18	NEEDHAM, BRADFORD H., ET AL.	
	3	20040103283		2004-05-27	HOMAK, ZOLTAN	
	4	20040101138		2004-05-27	REVITAL, DAN, ET AL.	
	5	20040091111		2004-05-13	LEVY, KENNETH L., ET AL.	
	6	20040073568		2004-04-15	YONAHA, MAKOTO	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	7	20040073557		2004-04-15	PICCIONELLI, GREGORY A., ET AL.	
	8	20040068371		2004-04-08	ESTEP, RANDALL S.	
	9	20040053637		2004-03-18	IIDA, TAKAYUKI	
	10	20040049734		2004-03-11	SIMSKE, STEVEN J.	
	11	20040044911		2004-03-04	TAKADA, MASAYUKI	
	12	20040039930		2004-02-26	OHMORI, MOTOJI, ET AL.	
	13	20040032499		2004-02-19	SILVERBROOK, KIA, ET AL.	
	14	20040023686		2004-02-05	KING, JOHN J., ET AL.	
	15	20040005078		2004-01-08	TILLOTSON, SCOTT ANDREW	
	16	20040022444		2004-02-05	RHOADS, GEOFFREY B.	
	17	20020073056		2002-06-13	BROSTER, IAN, ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	18	20010012062		2001-08-09	ANDERSON	
	19	20020191087		2002-12-19	HASHIMOTO, ET AL.	
	20	20030048921		2003-03-13	CAHALL, NATHAN D.	
	21	20020194480		2002-12-19	NAGAO, KATASHI	
	22	20030011684		2003-01-16	NARAYANASWAMI ET AL.	
	23	20030032033		2003-02-13	ANGLIN ET AL.	
	24	20050043018		2005-02-24	KAWAMOTO, YOJI	
	25	20060018506		2006-01-26	RODRIGUEZ ET AL.	
	26	20070055689		2007-03-08	RHOADS ET AL.	
	27	20010007130		2001-07-05	TAKARAGI	
	28	20010011680		2001-08-09	SOLTESZ ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	29	20010025342		2001-09-27	UCHIDA	
	30	20010034835		2001-10-25	SMITH	
	31	20020010684		2002-01-24	MOSKOWITZ	
	32	20020061120		2002-05-23	CARR ET AL.	
	33	20020072935		2002-06-13	ROWSE ET AL.	
	34	20010015759		2001-08-23	SQUIBBS	
	35	20010012066		2001-08-09	PARULSKI ET AL.	
	36	20010018349		2001-08-30	KINNUNEN ET AL.	
	37	20020046188		2002-04-18	BURGES ET AL.	
	38	20040197013		2004-10-07	KAMEI	
	39	20050134703		2005-06-23	MITTAL	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	40	20070250526		2007-10-25	HANNA	
	41	20070098172		2007-05-03	LEVY ET AL.	
	42	20030187950		2003-10-02	RISING III	
	43	20050231752		2005-10-20	SAINIO, KARI	
	44	20050219359		2005-10-06	TRELA, RICHARD STEVEN	
	45	20050216949		2005-09-29	CANDELORA ET AL.	
	46	20050216580		2005-09-29	RAJI ET AL.	
	47	20050185049		2005-08-25	IWAI ET AL.	
	48	20050143136		2005-06-30	LEV ET AL.	
	49	20050094000		2005-05-05	SON ET AL.	
	50	20050091311		2005-04-28	LUND ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	51	20050041035		2005-02-24	NAGATOMO ET AL.	
	52	20050024493		2005-02-03	NAM, KI Y.	
	53	20040257431		2004-12-23	GIRISH ET AL.	
	54	20040203386		2004-10-14	TISCHER ET AL.	
	55	20040183915		2004-09-23	GOTOHDA, ET AL.	
	56	20040148518		2004-07-29	GRUNDBACK ET AL.	
	57	20040109199		2004-06-10	TSUBAKI, HISAYOSHI	
	58	20040085203		2004-05-06	JUNQUA, JEAN-CLAUDE	
	59	20040070670		2004-04-15	FOSTER, WARD S.	
	60	20010021144		2001-09-13	OSHIMA ET AL.	
	61	20010021978		2001-09-13	OKAYASU ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	62	20010044824		2001-11-22	HUNTER ET AL.	
	63	20020001395		2002-01-03	DAVIS ET AL.	
	64	20020015042		2002-02-07	ROBOTHAM ET AL.	
	65	20020030907		2002-03-14	IKEDA ET AL.	
	66	20020031240		2002-03-14	LEVY ET AL.	
	67	20020032502		2002-03-14	RUSSELL, J. CHRIS	
	68	20020033844		2002-03-21	LEVY ET AL.	
	69	20020051577		2002-05-02	KINJO, NAOTO	
	70	20020059162		2002-05-16	SHINODA ET AL.	
	71	20020062382		2002-05-23	RHOADS ET AL.	
	72	20020075298		2002-06-20	SCHENA ET AL.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	73	20020080271		2002-06-27	EVELEENS ET AL.	
	74	20020080396		2002-06-27	SILVERBROOK ET AL.	
	75	20020080964		2002-06-27	STONE ET AL.	
	76	20020083123		2002-06-27	FREEDMAN ET AL.	
	77	20020102966		2002-08-01	LEV ET AL.	
	78	20020146148		2002-10-10	LEVY, KENNETH L.	
	79	20020152388		2002-10-17	LINNARTZ ET AL.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	0905966	EP		1999-03-31	CANON KABUSHIKI KAISHA		
	2	0152178	WO		2001-07-19	DIGIMARC CORPORATION		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

	3	9901859	WO		1999-01-14	IMIGE INCORPORATED		
	4	0167707	WO		2001-09-13	SCALE EIGHT, INCORPORATED		
	5	1204277	EP		2002-05-08	TEKTRONIX, INC.		
	6	9743736	WO		1997-11-20	DIGIMARC CORPORATION		
	7	9626494	WO		1996-08-29	THE REGENTS OF THE UNIVERSITY OF CALIFORNIA		
	8	9936876	WO		1999-07-22	DIGIMARC CORPORATION		
	9	0115021	WO		2001-03-01	DIGITAL CONVERGENCE.:COM INC.		
	10	0161508	WO		2001-08-23	DIGIMARC CORPORATION		
	11	0173586	WO		2001-10-04	DIGITAL: CONVERGENCE CORPORATION		
	12	0175629	WO		2001-10-11	NEOMEDIA TECHNOLOGIES, INC.		
	13	0197128	WO		2001-12-20	MARKANY INC.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	14	0211446	WO		2002-02-07	KONINKLIJKE PHILIPS ELECTRONICS, N.V.		
	15	9827510	WO		1998-06-25	THE REGENTS OF THE UNIVERSITY OF CALIFORNIA		
	16	0036605	WO		2000-06-22	KENT RIDGE DIGITAL LABS		
	17	0070585	WO		2000-11-23	DIGIMARC CORPORATION		
	18	9603286	WO		1996-02-08	INTERNATIONAL DATA MATRIX, INC.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,265; dated June 6, 2014; Examiner Angela M. Lie; 1085 pages 6 Jun 2014	
	2	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,255; dated May 27, 2014; Examiner Scott Louis Weaver; 906 pages 27 May 2014	
	3	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,265; dated February 16, 2015; Examiner Angela M. Lie; 187 pages 16 Feb 2015	
	4	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,255; dated March 2, 2015; Examiner Angela M. Lie; 177 pages 2 Mar 2015	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	5	H. KRAWCZYK, RFC 2104 (RFC2104) RFC 2104 - HMAC: Keyed-Hashing for Message Authentication https://www.faqs.org/rfcs/rfc2104.htm, February 1997.	
	6	G. Friedman, "The Trustworthy Digital Camera: Restoring Credibility To The Photographic Image," IEEE Transactions on Consumer Electronics, pages 905-910, Vol. 39, No. 4, November 1993.	
	7	FRANKS, et al., "HTTP Authentication: Basic and Digest Access Authentication," The Internet Society, June 1999.	
	8	FRANKS, et al., "An Extension to HTTP: Digest Access Authentication," The Internet Society, January 1997.	
	9	Supplemental First Amended Complaint, MyPort IP, Inc. v. HTC Corporation, Civil Action No. 6:11-cv-00246 (E.D. Tex. Filed March 8, 2012) ("MyPort Complaint"), 12 pages. 8 Mar 2012	
	10	Digital Still Camera Image File Format Standard (Exchangeable image file format for Digital Still Cameras: Exif), Version 2.1, published June 12, 1998 by the Japan Electronic Industry Development Association (JEIDA) ("Exif 2.1 Specification"), 173 pages.	
	11	TIFF Specification Revision 6.0, Aldus Developers Desk, Aldus Corporation, June 3, 1992.	
	12	James Bao-Yen Tsui, Fundamental of Global Positioning System Receivers: A Software Approach, pages 1-6, 73-108, 1983-217 (John Wiley & Sons, Inc. 2000).	
	13	PPP Encryption Control Protocol, Internet Engineering Task Force (IETF), published June 1996.	
	14	Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography (CRC Press 1996).	
	15	MyPort IP, Inc.'s Disclosure Pursuant to Patent Rule 3-1, MyPort IP, Inc. v. HTC Corporation, Civil Action No. 6:11-cv-00246 (E.D. Tex. Filed May 13, 2011).	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	16	STANSELL, Jr., "Civil GPS from a Future Perspective," Proceedings of the IEEE, October 1983, vol. 71, No. 10; pgs. 1187-1192. 1 Oct 1983	
	17	DALE, DIANA & ROG, RON, The Need For a Meta-Tag Standard for Audio and Visual Materials, Proc. Int. Conf. on Dublin Core and Metadata for e-Communities 2002: 205-206. 1 Jan 2002	
	18	KOSOVIC, DOUGLAS; SCHROETER, RONALD; and HUNTER, JANE, Collaborative Video Annotation, Indexing and Discussion over high-bandwidth networks, DSTC Technical Report TR247, 2002, DSTC Pty Ltd., St Lucia, Qld, Australia. 1 Jan 2002	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ISHRAT I SHERALI/	Date Considered	11/05/2018

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith D. Harden, Reg. # 74472/	Date (YYYY-MM-DD)	2018-04-23
Name/Print	Keith D. Harden	Registration Number	74472

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5267042		1993-11-30	TSUCHIYA ET AL.	
	2	6947571		2005-09-20	RHOADS ET AL.	
	3	6807534		2004-10-19	ERICKSON	
	4	6788800		2004-09-07	CARR ET AL	
	5	6786397		2004-09-07	SILVERBROOK ET AL	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button [Add]

NON-PATENT LITERATURE DOCUMENTS [Remove]

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button [Add]

EXAMINER SIGNATURE

Examiner Signature	/ISHRAT I SHERALI/	Date Considered	11/05/2018

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith D. Harden, Reg. # 74472/	Date (YYYY-MM-DD)	2018-04-23
Name/Print	Keith D. Harden	Registration Number	74472

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /I.I.S/

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	15824087
Filing Date	28-Nov-2017
First Named Inventor	Michael Malone
Attorney Docket Number	MPOR60-33823
Title of Invention	APPARATUS FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/ OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAG(S)/ CONTEXTUAL TAG(S), STORAGE AND SEARCH RETRIEVAL

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
MYPORT IP, INC.	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

7778438

9832017

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request. ○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.	
Applicant claims the following fee status: ○ Small Entity ○ Micro Entity ◉ Regular Undiscounted I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.	
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application Registration Number 30646 ○ A sole inventor ○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ○ A joint inventor; all of whom are signing this request	
Signature	/Gregory M. Howison, Reg. #30646/
Name	/Gregory M. Howison, Reg. #30646/

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	15824087
Filing Date:	28-Nov-2017
Title of Invention:	APPARATUS FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/ VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAG (S)/ CONTEXTUAL TAG(S), STORAGE AND SEARCH RETRIEVAL
First Named Inventor/Applicant Name:	Michael F. Malone
Filer:	Gregory Michael Howison
Attorney Docket Number:	MPOR60-33823

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 15824087

Filing Date: 28-Nov-2017

Applicant/Patent under Reexamination: Malone

Electronic Terminal Disclaimer filed on November 2, 2018

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	34201332
Application Number:	15824087
International Application Number:	
Confirmation Number:	5197
Title of Invention:	APPARATUS FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/ VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAG (S)/ CONTEXTUAL TAG(S), STORAGE AND SEARCH RETRIEVAL
First Named Inventor/Applicant Name:	Michael F. Malone
Customer Number:	25883
Filer:	Gregory Michael Howison
Filer Authorized By:	
Attorney Docket Number:	MPOR60-33823
Receipt Date:	02-NOV-2018
Filing Date:	28-NOV-2017
Time Stamp:	16:59:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$160
RAM confirmation Number	110518INTEFSW00003760200780
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	33785 5ae787c4c11c5ff613aeca177ac25a8b58e7d8e5	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30846 fb7bf903bf33c79458147512fa7d91d8c9717fb9	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	64631		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Michael F. Malone
Serial No.:	15/824,087
Confirmation No.:	5197
Filed:	November 28, 2017
Group:	2667
Examiner:	Ishrat T. Sherali
For:	APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL TAGS, STORAGE AND SEARCH RETRIEVAL (as amended)

Mail Stop AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

SUPPLEMENTAL AMENDMENT

This communication is supplemental to the Response filed on September 9, 2018. Reconsideration is respectfully requested.

Amendments to the Claims are reflected in the listing of claims beginning on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

Electronic Acknowledgement Receipt

EFS ID:	34201445
Application Number:	15824087
International Application Number:	
Confirmation Number:	5197
Title of Invention:	APPARATUS FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/ VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAG (S)/ CONTEXTUAL TAG(S), STORAGE AND SEARCH RETRIEVAL
First Named Inventor/Applicant Name:	Michael F. Malone
Customer Number:	25883
Filer:	Gregory Michael Howison
Filer Authorized By:	
Attorney Docket Number:	MPOR60-33823
Receipt Date:	02-NOV-2018
Filing Date:	28-NOV-2017
Time Stamp:	16:57:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		MPO33823SUPAMD.pdf	103183 675d889ee6ab9755035eea006a1e7a850d1962f2	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Applicant Arguments/Remarks Made in an Amendment	7	7
	Claims	2	6
	Supplemental Response or Supplemental Amendment	1	1
Warnings:			
Information:			
	Total Files Size (in bytes):	103183	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

REMARKS

Applicant has carefully reviewed the Office Action dated March 8, 2018. Applicant has amended claims 21, 25, 26, 30, 32, and 33. Reconsideration and favorable action is respectfully requested.

Applicant has now made an earnest attempt in order to place this case in condition for allowance. For the reasons stated above, Applicant respectfully requests full allowance of the claims as amended. Please charge any additional fees or deficiencies in fees or credit any overpayment to Deposit Account No. 20-0780/MPOR60-33823.

Respectfully submitted,
MUNCK WILSON MANDALA, LLP
Attorneys for Applicant

/Gregory M. Howison, Reg. #30646/

Gregory M. Howison
Registration No. 30,646

GMH/alb

P.O. Drawer 800889
Dallas, Texas 75380
Tel: 972-628-3600
Fax: 972-628-3616
November 2, 2018

In the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-20. (Canceled)

21. (Currently Amended) A system for capturing image and audio information for storage in a database at a location on a network, comprising:

a microphone interfaceable ~~interfacable~~ with an external audio information source that generates external audio information and a first data converter for capturing the ~~first~~ external audio information from the microphone,

a camera interfacing with an external image source to capture an image therefrom;

the first data converter processing the captured external audio information and storing it in a first digital audio format as stored digital audio within the capture device, the camera for processing the captured image and storing it as a stored digital image;

a data capture device for capturing, as captured data, location information and time information associated with at least the capture of the image and storing the captured data as stored captured data;

a data combiner for combining the stored digital audio, stored digital image and stored captured data as a composite data set;

an encryptor for encrypting the composite data set as an encrypted composite data set;

a transmitter for transmitting the encrypted composite data set ~~stored digital audio and stored digital image~~ to the location on the network; and

a system disposed at the location on the network and including:

a receiver for receiving the transmitted encrypted composite data set ~~digital audio and digital image~~ from the transmitter,

a decryptor decrypting the received encrypted composite data set as a decrypted composite data set to provide the decrypted composite data set as a received set of decrypted captured information,

a system data converter for converting the received digital audio in the decrypted composite data set to a text based searchable file as a text context tag and creating an image recognition searchable context tag with image recognition

of at least a portion of the digital image in the decrypted composite data set and associating the text and image recognition context tags with the digital image in the received decrypted composite data set, and

the database storing the digital image in the decrypted composite data set in association with the text and image recognition context tags as a stored context based digital image and in association with the received captured data in the decrypted composite data set.

22. (Previously Presented) The system of Claim 21, wherein the first data converter captures the first external audio information from the microphone during generation thereof.

23. (Previously Presented) The system of Claim 21, wherein the camera captures the image from the external image source at an instant in time.

24. (Previously Presented) The system of Claim 21, wherein the first data converter processes the captured external audio information from a start event representing the time that capture of the external audio information is initiated to a stop event representing the time that capture of the external audio information is complete.

25. (Currently Amended) The system of Claim 24, wherein the transmitter transmits the encrypted composite data set ~~stored digital audio information and the stored digital image~~ to the location on the network after at least the stop event associated with the processing of the captured external audio information.

26. (Currently Amended) A system for capturing image and audio information for storage, comprising:

a capture device having:

internal storage;

a microphone interfaceable ~~interfacable~~ with and external audio information source that generates external audio information and a first data converter for capturing the first external audio information from the microphone,

a camera interfacing with and external image source to capture an image therefrom;

the first data converter processing the captured external audio information and storing it in a first digital audio format as stored digital audio in internal storage within the capture device, the camera for processing the captured image and storing it as a stored digital image in internal storage; ~~and a combiner for~~

a data capture device for capturing, as captured data, location information, and time information associated with at least the capture of the image and storing the captured data as stored captured data;

~~generating an association between the stored digital audio and the stored digital image,~~

a media data converter for converting the ~~received set of captured information to convert~~ the received digital audio to a text based searchable file as a text context tag and creating an image recognition searchable context tag with image recognition of at least a portion of the digital image and associating the text and image recognition context tags with the digital image and the captured data, and

the internal storage storing the digital image in association with the text and image recognition context tags in addition to the stored captured data.

27. (Previously Presented) The system of Claim 26, wherein the first data converter captures the first external audio information from the microphone during generation thereof.

28. (Previously Presented) The system of Claim 26, wherein the camera captures the image from the external image source at an instant in time.

29. (Previously Presented) The system of Claim 26, wherein the first data converter processes the captured external audio information from a start event representing the time that capture of the external audio information is initiated to a stop event representing the time that capture of the external audio information is complete.

30. (Currently Amended) The system of Claim 26, and further including:

a transmitter associated with the capture device for transmitting the composite data set ~~associated stored digital image in association with the text and image recognition context tags~~ to the location on the network;

a system disposed at the location on a network and including:

a receiver for receiving the transmitted composite data set ~~associated stored digital image in association with the text and image recognition context tags~~ from the transmitter associated with the capture device as a received set of captured information,

a database, and

the database storing the received composite data set ~~associated stored digital image in association with the text and image recognition context tags~~.

31. (Previously Presented) The system of Claim 30, wherein the first data converter processes the captured external audio information from a start event representing the time that capture of the external audio information is initiated to a stop event representing the time that capture of the external audio information is complete.

32. (Currently Amended) The system of Claim 31, wherein the transmitter transmits the received composite data set ~~associated stored digital image in association with the text and image recognition context tags~~ to the location on the network after at least the stop event associated with the processing of the captured external audio information.

33. (Currently Amended) A system for capturing image and audio information for storage, comprising:

internal storage;

a microphone interfaceable ~~interfacable~~ with an external audio information source that generates external audio information and a first data converter for capturing the ~~first~~ external audio information from the microphone;

a camera interfacing with an image source to capture an image therefrom;

a data capture device for capturing, as captured data, location information and time information associated with at least the capture of the image and storing the captured data as stored captured data;

the first data converter processing the captured external audio information and storing it in a first digital audio format as stored digital audio within the capture device, the camera for processing the captured image and storing it as a stored digital image;

a second data converter for converting the received digital audio to a text based searchable file as a text context tag and creating an image recognition searchable context tag with image recognition of at least a portion of the digital image and associating the text and image recognition context tags with the digital image and with the stored captured data; and

the internal storage storing the digital image in association with the text and image recognition context tags in addition to the stored captured data.

34. (Previously Presented) The system of Claim 33, wherein the image source is an external image source.

35. (Previously Presented) The system of Claim 33, wherein the first data converter captures the first external audio information from the microphone during generation thereof.

36. (Previously Presented) The system of Claim 33, wherein the camera captures the image from the image source at an instant in time.

37. (Previously Presented) The system of Claim 33, wherein the first data converter processes the captured external audio information from a start event representing the time that capture of the external audio information is initiated to a stop event representing the time that capture of the external audio information is complete.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Michael F. Malone
Serial No.:	15/824,087
Confirmation No.:	5197
Filed:	November 28, 2017
Group:	2667
Examiner:	Ishrat T. Sherali
For:	APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL TAGS, STORAGE AND SEARCH RETRIEVAL (as amended)

Mail Stop AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

AMENDMENT AND RESPONSE TO OFFICE ACTION

This communication is responsive to the Examiner's Office Action dated March 8, 2018. Reconsideration is respectfully requested.

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Claims are reflected in the listing of claims beginning on page 3 of this paper.

Remarks/Arguments begin on page 7 of this paper.

In the Specification

Please replace the title with the following amended title:

APPARATUS FOR ~~PERSONAL~~ VOICE ASSISTANT, LOCATION TAGGING~~SERVICES~~, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL TAGS~~METATAG(S)/ CONTEXTUAL TAG(S)~~, STORAGE AND SEARCH RETRIEVAL

In the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-20. (Canceled)

21. (New) A system for capturing image and audio information for storage in a database at a location on a network, comprising:

a microphone interfacable with an external audio information source that generates external audio information and a first data converter for capturing the first external audio information from the microphone,

a camera interfacing with an external image source to capture an image therefrom;

the first data converter processing the captured external audio information and storing it in a first digital audio format as stored digital audio within the capture device, the camera for processing the captured image and storing it as a stored digital image;

a transmitter for transmitting the stored digital audio and stored digital image to the location on the network; and

a system disposed at the location on the network and including:

a receiver for receiving the transmitted digital audio and digital image from the transmitter as a received set of captured information,

a system data converter for converting the received digital audio to a text based searchable file as a text context tag and creating an image recognition searchable context tag with image recognition of at least a portion of the digital image and associating the text and image recognition context tags with the digital image, and

the database storing the digital image in association with the text and image recognition context tags.

22. (New) The system of Claim 21, wherein the first data converter captures the first external audio information from the microphone during generation thereof.

23. (New) The system of Claim 21, wherein the camera captures the image from the external image source at an instant in time.

24. (New) The system of Claim 21, wherein the first data converter processes the captured external audio information from a start event representing the time that capture of the external audio information is initiated to a stop event representing the time that capture of the external audio information is complete.

25. (New) The system of Claim 24, wherein the transmitter transmits the stored digital audio information and the stored digital image to the location on the network after at least the stop event associated with the processing of the captured external audio information.

26. (New) A system for capturing image and audio information for storage, comprising:

a capture device having:

internal storage;

a microphone interfacable with and external audio information source that generates external audio information and a first data converter for capturing the first external audio information from the microphone,

a camera interfacing with and external image source to capture an image therefrom;

the first data converter processing the captured external audio information and storing it in a first digital audio format as stored digital audio in internal storage within the capture device, the camera for processing the captured image and storing it as a stored digital image in internal storage and a combiner for generating an association between the stored digital audio and the stored digital image,

a media data converter for converting the received set of captured information to convert the received digital audio to a text based searchable file as a text context tag and creating an image recognition searchable context tag with image recognition of at least a portion of the digital image and associating the text and image recognition context tags with the digital image, and

the internal storage storing the digital image in association with the text and image recognition context tags.

27. (New) The system of Claim 26, wherein the first data converter captures the first external audio information from the microphone during generation thereof.

28. (New) The system of Claim 26, wherein the camera captures the image from the external image source at an instant in time.

29. (New) The system of Claim 26, wherein the first data converter processes the captured external audio information from a start event representing the time that capture of the external audio information is initiated to a stop event representing the time that capture of the external audio information is complete.

30. (New) The system of Claim 26, and further including:

a transmitter associated with the capture device for transmitting the associated stored digital image in association with the text and image recognition context tags to the location on the network;

a system disposed at the location on a network and including:

a receiver for receiving the transmitted associated stored digital image in association with the text and image recognition context tags from the transmitter associated with the capture device as a received set of captured information,

a database, and

the database storing the received associated stored digital image in association with the text and image recognition context tags.

31. (New) The system of Claim 30, wherein the first data converter processes the captured external audio information from a start event representing the time that capture of the external audio information is initiated to a stop event representing the time that capture of the external audio information is complete.

32. (New) The system of Claim 31, wherein the transmitter transmits the associated stored digital image in association with the text and image recognition context tags to the location on

the network after at least the stop event associated with the processing of the captured external audio information.

33. (New) A system for capturing image and audio information for storage, comprising:

internal storage;

a microphone interfacable with an external audio information source that generates external audio information and a first data converter for capturing the first external audio information from the microphone;

a camera interfacing with an image source to capture an image therefrom;

the first data converter processing the captured external audio information and storing it in a first digital audio format as stored digital audio within the capture device, the camera for processing the captured image and storing it as a stored digital image;

a second data converter for converting the received digital audio to a text based searchable file as a text context tag and creating an image recognition searchable context tag with image recognition of at least a portion of the digital image and associating the text and image recognition context tags with the digital image; and

the internal storage storing the digital image in association with the text and image recognition context tags.

34. (New) The system of Claim 33, wherein the image source is an external image source.

35. (New) The system of Claim 33, wherein the first data converter captures the first external audio information from the microphone during generation thereof.

36. (New) The system of Claim 33, wherein the camera captures the image from the image source at an instant in time.

37. (New) The system of Claim 33, wherein the first data converter processes the captured external audio information from a start event representing the time that capture of the external audio information is initiated to a stop event representing the time that capture of the external audio information is complete.

REMARKS

Applicant has carefully reviewed the Office Action dated March 8, 2018. Applicant has canceled Claims 1-20 and added new Claims 21-37. Reconsideration and favorable action is respectfully requested.

Claims 1-20 stand rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-12 of U.S. Patent No. 7,778,438. Applicant has canceled Claims 1-20 and added new Claims 21-37. Applicant therefore respectfully requests withdrawal of the nonstatutory obviousness-type double patenting rejection.

Claims 1-20 stand objected to because claims 1 and 20 are allegedly "directed toward data which is not any of the four eligible categories of invention." Applicant has canceled Claims 1-20 and added new Claims 21-37. Applicant respectfully submits that new Claims 21-37 overcome this objection and respectfully requests withdrawal of this objection.

Applicant has now made an earnest attempt in order to place this case in condition for allowance. For the reasons stated above, Applicant respectfully requests full allowance of the claims as amended.

If any issues arise, or if the Examiner has any suggestions for expediting allowance of this Application, the Applicant respectfully invites the Examiner to contact the undersigned at the telephone number indicated below or at kharden@munckwilson.com.

Recognizing that Internet communications are not secure, Applicant hereby authorizes the USPTO to communicate with the undersigned and practitioners in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application by video conferencing, instant messaging, or electronic mail. Applicant understands that a copy of these communications will be made of record in the application file.

Applicant has now made an earnest attempt in order to place this case in condition for allowance. For the reasons stated above, Applicant respectfully requests full allowance of the claims as amended. Please charge any additional fees or deficiencies in fees or credit any overpayment to Deposit Account No. 20-0780/MPOR60-33823.

Respectfully submitted,
MUNCK WILSON MANDALA, LLP
Attorneys for Applicant

/Keith D. Harden, Reg. #74472/
Keith D. Harden
Registration No. 74,472

KDH/alb

P.O. Drawer 800889
Dallas, Texas 75380
Tel: 972-628-3600
Fax: 972-628-3616
September 10, 2018

PTO/AIA/22 (03-13)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): MPOR60-33823

Application Number: 15/824,087

Filed: November 28, 2017

For: APPARATUS FOR VOICE ASSISTANT, LOCATION TAGGING, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAGS/CONTEXTUAL TAGS, STORAGE ,

Art Unit: 2667

Examiner: Ishrat T. Sherali

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 1400
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 200780.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 74,472.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Keith D. Harden, Reg. #74472/ — Signature

September 10, 2018 — Date

Keith D. Harden — Typed or printed name

972-628-3600 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of ONE forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	15824087
Filing Date:	28-Nov-2017
Title of Invention:	APPARATUS FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/ VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAG (S)/ CONTEXTUAL TAG(S), STORAGE AND SEARCH RETRIEVAL
First Named Inventor/Applicant Name:	Michael F. Malone
Filer:	Keith D. Harden
Attorney Docket Number:	MPOR60-33823

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
		Total in USD ($)		**1400**

Electronic Acknowledgement Receipt

EFS ID:	33677960
Application Number:	15824087
International Application Number:	
Confirmation Number:	5197
Title of Invention:	APPARATUS FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH TO TEXT CONVERSION, PHOTO/ VIDEO IMAGE/OBJECT RECOGNITION, CREATION OF SEARCHABLE METATAG (S)/ CONTEXTUAL TAG(S), STORAGE AND SEARCH RETRIEVAL
First Named Inventor/Applicant Name:	Michael F. Malone
Customer Number:	25883
Filer:	Keith D. Harden
Filer Authorized By:	
Attorney Docket Number:	MPOR60-33823
Receipt Date:	10-SEP-2018
Filing Date:	28-NOV-2017
Time Stamp:	18:50:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1400
RAM confirmation Number	091118INTEFSW00006244200780
Deposit Account	200780
Authorized User	Keith Harden
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		MPO33823AMD.pdf	100484 9f5e43c6e56df17dd0ffd69c797fc573a2b04be3	yes	8

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Specification	2	2
Claims	3	6
Applicant Arguments/Remarks Made in an Amendment	7	8

Warnings:					
Information:					
2	Extension of Time	MPO33823EXT.pdf	154612 9fc83be37f921384599b08cbedb09fe70f5a4914	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31248 a4d4f7fa4f881f570075318fa133f850333ad210	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	286344		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/824,087	Filing Date 11/28/2017	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	09/10/2018	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 17	Minus	** 20	= 0	X $100 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
MARTHA NEWMAN

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/824,087	Filing Date 11/28/2017	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 = *		X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 = *		X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 09/10/2018

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 17	Minus	** 20	= 0	X $100 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $460 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
MARTHA NEWMAN

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8424227		2013-04-23	HARRINGTON, JOHN	
	2	8099772		2012-01-17	TAKADA ET AL.	
	3	6968453		2005-11-22	DOYLE ET AL.	
	4	6996251		2006-02-07	MALONE ET AL.	
	5	4742369		1988-05-03	ISHII ET AL.	
	6	5031122		1991-07-09	WITTY	
	7	5276472		1994-01-04	BELL ET AL.	
	8	5546145		1996-08-13	BERNARDI ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	9	5786851		1998-07-28	KONDO ET AL.	
	10	5940121		1999-08-17	MCINTYRE ET AL.	
	11	5995936		1999-11-30	BRAIS ET AL.	
	12	6031526		2000-02-29	SHIPP	
	13	7617542		2009-11-10	VATAJA	
	14	6104430		2000-08-15	FUKUOKA	
	15	6683649		2004-01-27	ANDERSON	
	16	7053938		2006-05-30	SHERRY	
	17	7907199		2011-03-15	SEKI ET AL.	
	18	7831598		2010-11-09	KO	
	19	7324943		2008-01-29	RIGAZIO ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	20	7961218		2011-06-14	SEKI ET AL.	
	21	6115137		2000-09-05	OZAWA ET AL	
	22	6111605		2000-08-09	SUZUKI	
	23	7319484		2008-01-15	YOSHIDA ET AL	
	24	6222985		2001-04-24	MIYAKE	
	25	6741864		2004-05-25	WILCOCK, ET AL.	
	26	6636158		2003-10-21	BANDO, ET AL.	
	27	6525768		2003-02-25	OBRADOVICH	
	28	6720879		2004-04-03	EDWARDS	
	29	6507371		2003-01-14	HASHIMOTO, ET AL.	
	30	6498586		2002-12-24	PANKINAHO	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	31	6292633		2001-09-18	NAKAGAWA	
	32	6198989		2001-03-06	TANKHILEVICH, ET AL.	
	33	5768640		1998-06-16	TAKAHASHI, ET AL.	
	34	5642285		1997-06-24	WOO, ET AL.	
	35	6560660		2003-05-06	FLANAGIN	
	36	6526351		2003-02-25	WHITHAM	
	37	6160964		2000-12-12	IMOTO	
	38	6532298		2003-03-11	CAMBIER, ET AL.	
	39	6205249		2001-03-20	MOSKOWITZ	
	40	6185683		2001-02-06	GINTER, ET AL.	
	41	6714778		2004-03-30	NYKANEN, ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	42	6166729		2000-12-26	ACOSTA, EDWARD	
	43	6424968		2002-07-23	BROSTER, ET AL.	
	44	6065119		2000-05-16	SANDFORD, II, ET AL.	
	45	6462778		2002-10-08	ABRAM, ET AL.	
	46	6505160		2003-01-07	LEVY, ET AL.	
	47	6526215		2003-02-25	HIRAI, ET AL.	
	48	6606117		2003-08-12	WINDLE	
	49	2950971		1960-08-30	LEWIN	
	50	3439598		1969-04-22	WEITZNER, ET AL.	
	51	5602458		1997-02-11	DOWE	
	52	5692225		1997-11-25	BERNARDI, ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	53	6681029		2004-01-20	RHOADS	
	54	7010144		2006-03-07	DAVIS ET AL.	
	55	7043048		2006-05-09	ELLINGSON	
	56	0055422		1866-06-05	ROUSTAEI	
	57	4015240		1977-03-29	SWONGER ET AL.	
	58	4109237		1978-08-22	HILL	
	59	4528588		1985-07-09	LOFBERG	
	60	4620318		1986-10-28	HILL	
	61	4994831		1991-02-19	MARANDI	
	62	4995086		1991-02-19	LILLEY ET AL.	
	63	5103486		1992-04-07	GRIPPI	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	64	5767496		1998-06-16	SWARTZ ET AL.	
	65	5787183		1998-07-28	SCHROEDER	
	66	5799092		1998-08-25	KRISTOL ET AL.	
	67	5841886		1998-11-24	RHOADS	
	68	5857038		1999-01-05	OWADA ET AL.	
	69	5907149		1999-05-25	MARCKINI	
	70	5995630		1999-11-30	BORZA	
	71	6005936		1999-12-21	SCHIMIZU ET AL.	
	72	6064764		2000-05-16	BHASKARAN ET AL.	
	73	6148091		2000-11-24	DIMARIA	
	74	6185316		2001-02-06	BUFFAM	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	75	6208746		2001-03-27	MUSGRAVE	
	76	6243481		2001-06-05	TAO	
	77	6292092		2001-09-18	CHOW ET AL.	
	78	6301368		2001-10-09	BOLLE ET AL.	
	79	6321981		2001-11-27	RAY ET AL.	
	80	6366680		2002-04-02	BRUNK ET AL.	
	81	6377699		2002-04-23	MUSGRAVE ET AL.	
	82	6389151		2002-05-14	CARR ET AL.	
	83	6397334		2002-05-28	CHAINER ET AL.	
	84	6577336		2003-06-10	SAFAI	
	85	6687383		2004-02-03	KANEVSKY ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	86	7778440		2010-08-17	MALONE, MICHAEL F.	
	87	8068638		2011-11-29	MALONE, MICHAEL F.	
	88	7184573		2007-02-27	MALONE ET AL.	
	89	6023241		2000-02-08	CLAPPER	
	90	5913078		1999-06-15	KIMURA ET AL.	
	91	5732354		1998-03-24	MACDONALD	
	92	6212401		2001-04-03	ACKLEY	
	93	5825890		1998-10-20	ELGAMAL ET AL.	
	94	8135169		2012-03-13	MALONE, MICHAEL F.	
	95	6914695		2005-07-05	WALTERS ET AL.	
	96	5247300		1993-09-21	SOHN, SUNG W.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	97	7778438		2010-08-17	MALONE, MICHAEL F.	
	98	RE39526		2007-03-20	HULL ET AL.	
	99	52670425		1993-11-30	TSUCHIYA ET AL.	
	100	5515042		1996-05-07	NELSON	
	101	5712679		1998-01-27	COLES	
	102	5726660		1998-03-10	PURDY ET AL.	
	103	5806005		1998-09-08	HULL ET AL.	
	104	6181373		2001-01-30	COLES	
	105	6359837		2002-03-19	TSUKAMOTO	
	106	6571271		2003-05-27	SAVITZKY ET AL.	
	107	6831682		2004-12-14	SILVERBROOK ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	108	6833861		2004-12-21	MATSUMOTO ET AL.	
	109	7016899		2006-03-21	STERN ET AL.	
	110	7265779		2007-09-04	SATO ET AL.	
	111	6889324		2005-05-03	KANAI ET AL.	
	112	6853987		2005-02-08	COOK, DAVID P.	
	113	6269446		2001-07-31	SCHUMACHER ET AL.	
	114	6968366		2005-11-22	ZHANG ET AL.	
	115	7391960		2008-06-24	SHINOZAKI ET AL.	
	116	6990444		2006-01-24	HIND ET AL.	
	117	5737491		1998-04-07	ALLEN ET AL.	
	118	4115805		1978-09-19	MORTON	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	119	4334241		1982-06-08	KASHIOKA, ET AL.	
	120	4574319		1986-03-04	KONISHI	
	121	5335072		1994-08-02	TANAKA, ET AL.	
	122	5506644		1996-04-09	SUZUKI, ET AL.	
	123	5633678		1997-05-27	PARULSKI, ET AL.	
	124	6332193		2001-12-18	GLASS, ET AL.	
	125	6219560		2001-04-17	ERKKILA, MARKO	
	126	6014183		2000-01-11	HOANG	
	127	6115717		2000-09-05	MEHROTRA ET AL.	
	128	5819289		1998-10-06	SANFORD, II ET AL.	
	129	5657077		1997-08-12	DEANGELIS, ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	130	5682458		1997-10-28	FUNAZAKI	
	131	5692104		1997-11-25	CHOW, ET AL.	
	132	5706457		1998-01-06	DWYER, ET AL.	
	133	5796428		1998-08-18	MATSUMOTO, ET AL.	
	134	5828809		1998-10-27	CHANG, ET AL.	
	135	5835667		1998-11-10	WACTLAR, ET AL.	
	136	5872865		1999-02-16	NORMILE, ET AL.	
	137	5889578		1999-03-30	JAMZADEH	
	138	5893095		1999-04-06	JAIN, ET AL.	
	139	6282362		2001-08-28	MURPHY, ET AL.	
	140	5499294		1996-03-12	FRIEDMAN, GARY L.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	141	5815201		1998-09-29	HASHIMOTO ET AL.	
	142	4389109		1983-06-21	TANIGUCHI ET AL.	
	143	4270853		1981-06-02	HATADA ET AL.	
	144	4270854		1981-06-02	STEMME ET AL.	
	145	4344682		1982-08-17	HATTORI	
	146	4443077		1984-04-17	TANIKAWA	
	147	4613911		1986-09-23	OHTA	
	148	4642717		1987-02-10	MATSUDA ET AL.	
	149	4905029		1990-02-27	KELLEY	
	150	4951079		1990-08-21	HOSHINO ET AL.	
	151	4965626		1990-10-23	ROBISON ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	152	4977419		1990-12-11	WASH ET AL.	
	153	4983996		1991-01-08	KINOSHITA	
	154	5023635		1991-06-11	NEALON	
	155	5025283		1991-06-18	ROBINSON	
	156	5027149		1991-06-25	HOSHINO ET AL.	
	157	5070355		1991-12-03	INOUE ET AL.	
	158	5097278		1992-03-17	TAMAMURA ET AL.	
	159	5099262		1992-03-24	TANAKA ET AL.	
	160	5128700		1992-07-07	INOUE ET AL.	
	161	5142310		1992-08-25	TANIGUCHI ET AL.	
	162	5146249		1992-09-08	HODA ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	163	5160952		1992-11-03	IWASHITA ET AL.	
	164	5245372		1993-09-14	OASHIMA	
	165	5313235		1994-05-17	INOUE ET AL.	
	166	5426745		1995-06-20	BAJI ET AL.	
	167	6952164		2005-10-04	JUNQUA	
	168	6959868		2005-11-01	TSIKOS ET AL.	
	169	6965324		2005-11-15	SUGGS, SR.	
	170	6956671		2005-10-18	MONTY ET AL.	
	171	6895126		2005-05-17	DI BERNARDO ET AL.	
	172	6856344		2005-02-15	FRANZ	
	173	6750902		2004-06-15	STEINBERG ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	174	6747692		2004-06-08	PATEL ET AL.	
	175	6670984		2003-12-30	TANAKA ET AL.	
	176	6628325		2003-12-30	STEINBERG ET AL.	
	177	6535298		2003-03-18	WINTER ET AL	
	178	6411328		2002-06-25	FRANKE ET AL.	
	179	7095871		2006-08-22	JONES ET AL.	
	180	5841978		1998-11-24	RHOADS	
	181	5410598		1995-04-25	SHEAR	
	182	5493677		1996-02-20	BALOGH ET AL.	
	183	5502576		1996-03-26	RAMSAY ET AL.	
	184	5519778		1996-05-21	LEIGHTON ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	185	5530759		1996-06-25	BRAUDAWAY ET AL.	
	186	5568570		1996-10-22	RABBANI	
	187	5581800		1996-12-03	FARDEAU ET AL.	
	188	5617119		1997-04-01	BRIGGS ET AL.	
	189	5629980		1997-05-13	STEFIK	
	190	5646990		1997-07-08	LI	
	191	5646997		1997-07-08	BARTSON	
	192	5740244		1998-04-14	INDECK ET AL.	
	193	5765152		1998-06-09	ERICKSON	
	194	5822432		1998-10-13	MOSKOWITZ ET AL.	
	195	5845281		1998-12-01	BENSON	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	196	5862260		1999-01-19	RHOADS	
	197	5892900		1999-04-06	GINTER ET AL.	
	198	5923327		1999-07-13	SMITH ET AL.	
	199	5943422		1999-08-24	VAN WIE ET AL.	
	200	5978773		1999-11-02	HUDETZ ET AL.	
	201	5991876		1999-11-23	JOHNSON ET AL.	
	202	6014569		2000-01-11	BOTTUM	
	203	6122403		2000-09-19	RHOADS	
	204	6141753		2000-10-31	ZHAO ET AL.	
	205	6233684		2001-05-15	STEFIK ET AL.	
	206	6243480		2001-06-05	ZHAO ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	207	6282654		2001-08-28	IKEDA ET AL.	
	208	6300880		2001-10-09	SITNIK	
	209	6334187		2001-12-25	KADONO	
	210	6363043		2002-03-26	KONDO	
	211	6389538		2002-05-14	GRUSE ET AL.	
	212	6421450		2002-07-16	NAKANO	
	213	6437933		2002-08-20	SUGIYAMA ET AL.	
	214	6449367		2002-09-10	VAN WIE ET AL.	
	215	6469969		2002-10-22	CARSON ET AL.	
	216	6491217		2002-12-10	CATAN	
	217	6560339		2003-05-06	IWAMURA	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	218	6591365		2003-07-08	COOKSON	
	219	6611607		2003-08-26	DAVIS ET AL	
	220	6636249		2003-10-21	REKIMOTO	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040114042		2004-06-17	PAOLINI, MICHAEL A., ET AL.	
	2	20030177094		2003-09-18	NEEDHAM, BRADFORD H., ET AL.	
	3	20040103283		2004-05-27	HOMAK, ZOLTAN	
	4	20040101138		2004-05-27	REVITAL, DAN, ET AL.	
	5	20040091111		2004-05-13	LEVY, KENNETH L., ET AL.	
	6	20040073568		2004-04-15	YONAHA, MAKOTO	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	7	20040073557		2004-04-15	PICCIONELLI, GREGORY A., ET AL.	
	8	20040068371		2004-04-08	ESTEP, RANDALL S.	
	9	20040053637		2004-03-18	IIDA, TAKAYUKI	
	10	20040049734		2004-03-11	SIMSKE, STEVEN J.	
	11	20040044911		2004-03-04	TAKADA, MASAYUKI	
	12	20040039930		2004-02-26	OHMORI, MOTOJI, ET AL.	
	13	20040032499		2004-02-19	SILVERBROOK, KIA, ET AL.	
	14	20040023686		2004-02-05	KING, JOHN J., ET AL.	
	15	20040005078		2004-01-08	TILLOTSON, SCOTT ANDREW	
	16	20040022444		2004-02-05	RHOADS, GEOFFREY B.	
	17	20020073056		2002-06-13	BROSTER, IAN, ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	18	20010012062		2001-08-09	ANDERSON	
	19	20020191087		2002-12-19	HASHIMOTO, ET AL.	
	20	20030048921		2003-03-13	CAHALL, NATHAN D.	
	21	20020194480		2002-12-19	NAGAO, KATASHI	
	22	20030011684		2003-01-16	NARAYANASWAMI ET AL.	
	23	20030032033		2003-02-13	ANGLIN ET AL.	
	24	20050043018		2005-02-24	KAWAMOTO, YOJI	
	25	20060018506		2006-01-26	RODRIGUEZ ET AL.	
	26	20070055689		2007-03-08	RHOADS ET AL.	
	27	20010007130		2001-07-05	TAKARAGI	
	28	20010011680		2001-08-09	SOLTESZ ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	29	20010025342		2001-09-27	UCHIDA	
	30	20010034835		2001-10-25	SMITH	
	31	20020010684		2002-01-24	MOSKOWITZ	
	32	20020061120		2002-05-23	CARR ET AL.	
	33	20020072935		2002-06-13	ROWSE ET AL.	
	34	20010015759		2001-08-23	SQUIBBS	
	35	20010012066		2001-08-09	PARULSKI ET AL.	
	36	20010018349		2001-08-30	KINNUNEN ET AL.	
	37	20020046188		2002-04-18	BURGES ET AL.	
	38	20040197013		2004-10-07	KAMEI	
	39	20050134703		2005-06-23	MITTAL	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	40	20070250526		2007-10-25	HANNA	
	41	20070098172		2007-05-03	LEVY ET AL.	
	42	20030187950		2003-10-02	RISING III	
	43	20050231752		2005-10-20	SAINIO, KARI	
	44	20050219359		2005-10-06	TRELA, RICHARD STEVEN	
	45	20050216949		2005-09-29	CANDELORA ET AL.	
	46	20050216580		2005-09-29	RAJI ET AL.	
	47	20050185049		2005-08-25	IWAI ET AL.	
	48	20050143136		2005-06-30	LEV ET AL.	
	49	20050094000		2005-05-05	SON ET AL.	
	50	20050091311		2005-04-28	LUND ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	51	20050041035		2005-02-24	NAGATOMO ET AL.	
	52	20050024493		2005-02-03	NAM, KI Y.	
	53	20040257431		2004-12-23	GIRISH ET AL.	
	54	20040203386		2004-10-14	TISCHER ET AL.	
	55	20040183915		2004-09-23	GOTOHDA, ET AL.	
	56	20040148518		2004-07-29	GRUNDBACK ET AL.	
	57	20040109199		2004-06-10	TSUBAKI, HISAYOSHI	
	58	20040085203		2004-05-06	JUNQUA, JEAN-CLAUDE	
	59	20040070670		2004-04-15	FOSTER, WARD S.	
	60	20010021144		2001-09-13	OSHIMA ET AL.	
	61	20010021978		2001-09-13	OKAYASU ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	62	20010044824		2001-11-22	HUNTER ET AL.	
	63	20020001395		2002-01-03	DAVIS ET AL.	
	64	20020015042		2002-02-07	ROBOTHAM ET AL.	
	65	20020030907		2002-03-14	IKEDA ET AL.	
	66	20020031240		2002-03-14	LEVY ET AL.	
	67	20020032502		2002-03-14	RUSSELL, J. CHRIS	
	68	20020033844		2002-03-21	LEVY ET AL.	
	69	20020051577		2002-05-02	KINJO, NAOTO	
	70	20020059162		2002-05-16	SHINODA ET AL.	
	71	20020062382		2002-05-23	RHOADS ET AL.	
	72	20020075298		2002-06-20	SCHENA ET AL.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	73	20020080271		2002-06-27	EVELEENS ET AL.	
	74	20020080396		2002-06-27	SILVERBROOK ET AL.	
	75	20020080964		2002-06-27	STONE ET AL.	
	76	20020083123		2002-06-27	FREEDMAN ET AL.	
	77	20020102966		2002-08-01	LEV ET AL.	
	78	20020146148		2002-10-10	LEVY, KENNETH L.	
	79	20020152388		2002-10-17	LINNARTZ ET AL.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	0905966	EP		1999-03-31	CANON KABUSHIKI KAISHA		
	2	0152178	WO		2001-07-19	DIGIMARC CORPORATION		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	3	9901859	WO		1999-01-14	IMIGE INCORPORATED		
	4	0167707	WO		2001-09-13	SCALE EIGHT, INCORPORATED		
	5	1204277	EP		2002-05-08	TEKTRONIX, INC.		
	6	9743736	WO		1997-11-20	DIGIMARC CORPORATION		
	7	9626494	WO		1996-08-29	THE REGENTS OF THE UNIVERSITY OF CALIFORNIA		
	8	9936876	WO		1999-07-22	DIGIMARC CORPORATION		
	9	0115021	WO		2001-03-01	DIGITAL CONVERGENCE.:COM INC.		
	10	0161508	WO		2001-08-23	DIGIMARC CORPORATION		
	11	0173586	WO		2001-10-04	DIGITAL: CONVERGENCE CORPORATION		
	12	0175629	WO		2001-10-11	NEOMEDIA TECHNOLOGIES, INC.		
	13	0197128	WO		2001-12-20	MARKANY INC.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	14	0211446	WO		2002-02-07	KONINKLIJKE PHILIPS ELECTRONICS, N.V.		
	15	9827510	WO		1998-06-25	THE REGENTS OF THE UNIVERSITY OF CALIFORNIA		
	16	0036605	WO		2000-06-22	KENT RIDGE DIGITAL LABS		
	17	0070585	WO		2000-11-23	DIGIMARC CORPORATION		
	18	9603286	WO		1996-02-08	INTERNATIONAL DATA MATRIX, INC.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,265; dated June 6, 2014; Examiner Angela M. Lie; 1085 pages 6 Jun 2014	
	2	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,255; dated May 27, 2014; Examiner Scott Louis Weaver; 906 pages 27 May 2014	
	3	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,265; dated February 16, 2015; Examiner Angela M. Lie; 187 pages 16 Feb 2015	
	4	United States Patent and Trademark Office; Request for Ex Parte Reexamination in related re-exam application 90/013,255; dated March 2, 2015; Examiner Angela M. Lie; 177 pages 2 Mar 2015	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	5	H. KRAWCZYK, RFC 2104 (RFC2104) RFC 2104 - HMAC: Keyed-Hashing for Message Authentication https://www.faqs.org/rfcs/rfc2104.htm, February 1997.	
	6	G. Friedman, "The Trustworthy Digital Camera: Restoring Credibility To The Photographic Image," IEEE Transactions on Consumer Electronics, pages 905-910, Vol. 39, No. 4, November 1993.	
	7	FRANKS, et al., "HTTP Authentication: Basic and Digest Access Authentication," The Internet Society, June 1999.	
	8	FRANKS, et al., "An Extension to HTTP: Digest Access Authentication," The Internet Society, January 1997.	
	9	Supplemental First Amended Complaint, MyPort IP, Inc. v. HTC Corporation, Civil Action No. 6:11-cv-00246 (E.D. Tex. Filed March 8, 2012) ("MyPort Complaint"), 12 pages. 8 Mar 2012	
	10	Digital Still Camera Image File Format Standard (Exchangeable image file format for Digital Still Cameras: Exif), Version 2.1, published June 12, 1998 by the Japan Electronic Industry Development Association (JEIDA) ("Exif 2.1 Specification"), 173 pages.	
	11	TIFF Specification Revision 6.0, Aldus Developers Desk, Aldus Corporation, June 3, 1992.	
	12	James Bao-Yen Tsui, Fundamental of Global Positioning System Receivers: A Software Approach, pages 1-6, 73-108, 1983-217 (John Wiley & Sons, Inc. 2000).	
	13	PPP Encryption Control Protocol, Internet Engineering Task Force (IETF), published June 1996.	
	14	Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography (CRC Press 1996).	
	15	MyPort IP, Inc.'s Disclosure Pursuant to Patent Rule 3-1, MyPort IP, Inc. v. HTC Corporation, Civil Action No. 6:11-cv-00246 (E.D. Tex. Filed May 13, 2011).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

	16	STANSELL, Jr., "Civil GPS from a Future Perspective," Proceedings of the IEEE, October 1983, vol. 71, No. 10; pgs. 1187-1192. 1 Oct 1983	
	17	DALE, DIANA & ROG, RON, The Need For a Meta-Tag Standard for Audio and Visual Materials, Proc. Int. Conf. on Dublin Core and Metadata for e-Communities 2002: 205-206. 1 Jan 2002	
	18	KOSOVIC, DOUGLAS; SCHROETER, RONALD; and HUNTER, JANE, Collaborative Video Annotation, Indexing and Discussion over high-bandwidth networks, DSTC Technical Report TR247, 2002, DSTC Pty Ltd., St Lucia, Qld, Australia. 1 Jan 2002	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith D. Harden, Reg. # 74472/	Date (YYYY-MM-DD)	2018-04-23
Name/Print	Keith D. Harden	Registration Number	74472

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15824087
Filing Date	2017-11-28
First Named Inventor	MALONE, Michael F.
Art Unit	2667
Examiner Name	SHERALI, Ishrat I.
Attorney Docket Number	MPOR60-33823

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5267042		1993-11-30	TSUCHIYA ET AL.	
	2	6947571		2005-09-20	RHOADS ET AL.	
	3	6807534		2004-10-19	ERICKSON	
	4	6788800		2004-09-07	CARR ET AL	
	5	6786397		2004-09-07	SILVERBROOK ET AL	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15824087
	Filing Date	2017-11-28
	First Named Inventor	MALONE, Michael F.
	Art Unit	2667
	Examiner Name	SHERALI, Ishrat I.
	Attorney Docket Number	MPOR60-33823

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Keith D. Harden, Reg. # 74472/	Date (YYYY-MM-DD)	2018-04-23
Name/Print	Keith D. Harden	Registration Number	74472

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 905 966 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
31.03.1999 Bulletin 1999/13

(51) Int Cl.[6]: **H04N 1/21**
// H04N101:00

(21) Application number: **98307925.2**

(22) Date of filing: **29.09.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **30.09.1997 JP 266616/97**
11.09.1998 JP 258182/98

(71) Applicant: **CANON KABUSHIKI KAISHA**
Tokyo (JP)

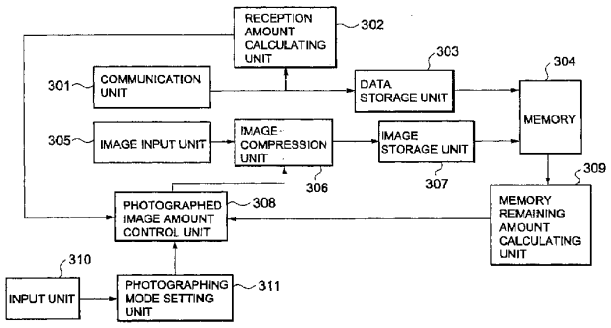
(72) Inventors:
- **Yoshida, Shigeo, Canon Kabushiki Kaisha**
  Ohta-ku, Tokyo (JP)
- **Sonobe, Hiraku, Canon Kabushiki Kaisha**
  Ohta-ku, Tokyo (JP)
- **Ono, Satoshi, Canon Kabushiki Kaisha**
  Ohta-ku, Tokyo (JP)
- **Ohara, Keiji, Canon Kabushiki Kaisha**
  Ohta-ku, Tokyo (JP)
- **Matsumoto, Shinichi, Canon Kabushiki Kaisha**
  Ohta-ku, Tokyo (JP)
- **Seki, Takayuki, Canon Kabushiki Kaisha**
  Ohta-ku, Tokyo (JP)

(74) Representative:
Beresford, Keith Denis Lewis et al
BERESFORD & Co.
2-5 Warwick Court
High Holborn
London WC1R 5DJ (GB)

(54) An image processing method, an image processing apparatus, an image input device, a photographing system, a communication device, a communication system, and a storage medium

(57) A method for processing images comprises the steps of performing the reception of data through the net work, inputting image data obtainable in accordance with the designated input mode, managing the storage of the data received in the receiving step and the image data inputted in the input step to the memory, and intervening between the operations of the reception step and the input step in accordance with the storage management in the controlling step. With the method thus structured, the compression ratio of the input image is heightened by changing the current photographing mode if the added value of the estimated reception data through communicating means and the data side of photographed image predetermined by the current photographing mode should exceed the remainders of memory in the storage, hence making it possible to implement the compatibility of immediacy between the image input and the communication by dealing with any sudden reception during photographing.

FIG.15



EP 0 905 966 A2

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates to a digital camera and the like. More particularly, the invention relates to an image input device, a photographing device, and photographing system, which are provided with communicating functions, and a communication device, and a communication system, which perform transmission and reception of images or the like. The invention also relates to a storage medium that stores processing steps readable by a computer for controlling the operations of the apparatuses, devices, or systems.

Related Background Art

[0002] Along with the technical advancement of semiconductor and others, the pluralization of digital cameras has been remarkable in recent years. The digital camera digitizes photographed images and stores them on the image memory. For an image memory of the kind, a semiconductor storage is often used in particular.

[0003] However, since the semiconductor storage is extremely expensive, there is automatically a limit as to the capacity of the semiconductor storage that may be adoptable for a digital camera in consideration of the overall costs of the digital camera to be used. In other words, the number of photographs that can be taken is limited. At present, the standard capacity of the semiconductor storage provided for a digital cameral is not large enough for the photographing frequency usually anticipated for a camera equipment.

[0004] Now, for example, there is a digital camera that uses an exchangeable storage device, such as a PCMCIA flash memory card, a smart memory, so that the number of photographs taken by such camera is increased by allowing the user to exchange the image storage in accordance with his requirement.

[0005] Conceivably, however, there is a case where no image storage is obtainable anew when the user wishes to replace the storage that has become full. As a result, the user should estimate the number of photographs that he may wish to take beforehand, and bring with him the PCMCIA flash memory cards or the like with a sufficient room for such estimated number.

[0006] Also, in order to secure the sufficient number of photographs that may be taken in anticipation of the general photographing frequency needed for the camera equipment described above, it may be possible to use some other media than the semiconductor storage, such as a hard disc or other magnetic storage.

[0007] Nevertheless, even if a magnetic storage is used as the image memory, its capacity is not infinite. There is naturally a limit to it.

[0008] Therefore, the number of photographs that may be taken by the aforesaid digital camera is confined depending on the capacity of the built-in image storage or the availability of the exchangeable storage device. Under such circumstances, if pictures should be taken on the photographing site in the numbers beyond such limit, for example, it is necessary to erase the unwanted pictures that have been taken and stored on the image storage or transfer the stored images to the storage device or the like in a personal computer. With an operation of the kind, it is possible to increase the capacity of the image storage for use.

[0009] However, the requirement of such operation as described above that should be carried out on the photographing site results in the time loss inevitably, and this becomes a significant drawback in using a digital camera for which immediacy is essential.

[0010] More specifically, when an unwanted picture should be erased from among the images that have been photographed, it is imperative to confirm various pieces of information to determine which one of them can be discarded. Making such confirmation exactly becomes a great burden on the photographer. In some cases, it is not easy to determine whether or not the photographed image is readily usable through the small display screen generally provided for a digital camera.

[0011] Further, in order to implement the aforesaid confirmation to be made efficiently, there is a need for the provision of a new group of operational switches or a display screen dedicated for the confirmation use. This may stand in the way of making the digital camera smaller.

[0012] Furthermore, it presents a psychological burden on the photographer eventually if any one of the images that he has taken should be erased on the photographing site. To such operation as described above, therefore, his sense of denial should be intense.

[0013] On the other hand, when the photographed images are transferred to the storage device in a personal computer, such burdens as described above are not imposed upon the photographer, but the interface or the like to perform such transfer between the digital camera and the personal computer should be carried around with the photographer. As a result, the physical burden becomes greater on his side.

Ex.1002 / Page 246 of 1385
APPLE INC.

[0014] Here, therefore, in order to solve the above problems, it is conceivable to provide a digital cameral with communicating functions, for example, so that the photographed images or electronic mails are transmitted or received as required.

[0015] Nevertheless, with a digital camera that may be structured to enable it to operate communications, the collision of requests may take place on a memory if one and the same memory is used to store photographed images and the data on transmission and reception. Then, there will be created the problem anew that may have not been encountered with the digital camera which is provided only with the photographing functions. For example, if the memory which is intended to be used for the storage of a photographed image should be occupied by the receiving data by the reception call of communication on the very moment the photographer is about to take a picture, the photographing which has been possible up to that moment is no longer executable.

[0016] In order to avoid a problem of the kind, the photographer is required to determine on the site whether or not such communication should be received on the moment a communication call is notified. Then, it becomes impossible to maintain the immediacy of photography, and there is a good possibility that a shutter chance is lost eventually. A problem of the kind presents a significant drawback in using a digital camera.

[0017] Also, it is conceivable that the reception data is not stored completely up to the end if the photographing function should operate while in communication. This may produce unfavorable effect on the reliability of communication. As a result, it may also present a significant drawback in using a digital camera which is provided with the communicating function.

SUMMARY OF THE INVENTION

[0018] The present invention is designed in consideration of the problems described above. It isa concern of the invention to solve all or at least one of the problems.

[0019] It is another concern of the invention to make the restrictions smaller on the functions of the apparatus due to the capacity of its storage.

[0020] It is still another concern of the invention to avoid marring the immediacy of image recording. It is a further object of the invention to provide an image input device, a photographing device, a communication device, a communication system, and a storage medium that stores the processing steps readable by a computer for the operational control of the apparatuses, devices, or systems, which make it possible to provide a digital camera whose performance is enhanced while being capable of maintaining its smallness and the immediacy of photography.

[0021] In accordance with an aspect of the present invention one embodiment thereof discloses a method for processing images comprising the steps of performing the reception of data through the net work; inputting image data obtained in accordance with the designated input mode; managing the storage of the data received in the receiving step and the image data inputted in the input step to the memory; and intervening between the operations of the reception step and the input step on the basis of the storage management in the managing step.

[0022] In this way, it becomes possible to deal with any sudden reception or the like during the storing operation of the image data on the memory, because the data reception operation and the image input operation can be controlled in accordance with the current status of memory storage. As a result, the compatibility of immediacy can be implemented between the image input and the communication.

[0023] Also, the aforesaid reception step further comprises the step of receiving data through wireless net work.

[0024] Thus, it is possible to deal with the communication through the wireless net work.

[0025] Also, the aforesaid intervening step further cbmprises the control step of controlling the input mode in the input step in accordance with the storage management in the management step.

[0026] In this way, it becomes possible to control the storing operation of the image data on the memory by changing the current input modes in accordance with the status of the memory storage.

[0027] Also, the aforesaid input step further comprises an image inreversible compression step, and the intervening step further comprises a control step for controlling the compression ratio in the compression step.

[0028] In this way, it becomes possible to control the amount of image data to be stored on the memory by changing the compression ratios in accordance with the status of the memory storage.

[0029] Moreover, the aforesaid management step further comprises a step of managing the remaining storage capacity of the memory.

[0030] Hence, it is possible to control the data reception operation and the image input operation in accordance with the remainders (remaining amount) of the storage capacity of the memory.

[0031] It is still another concern of the present invention to provide a photographing apparatus having new functions, a communicating device, or a storage medium for the execution of the functions of such apparatus by use of a computer.

[0032] Other features and advantages besides those discussed above will be apparent to those skilled in the art from the description of a preferred embodiment of the invention which follows. In the description, reference is made to accompanying drawings, which form a part hereof, and which illustrate an example of the invention. Such example,

Ex.1002 / Page 247 of 1385
APPLE INC.

however, is not exhaustive of the various embodiments of the invention, and therefore, reference is made to the claims which follow the description for determining the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0033] Fig. 1 is a view which shows the outer appearance of the front of a digital camera that executes a method for processing images in accordance with a first embodiment of the present invention.

[0034] Fig. 2 is a view which shows the outer appearance of the digital camera represented in Fig. 1, observed from the aspect other than the front side.

[0035] Fig. 3 is a view which illustrates the mode dials of the digital camera represented in Fig. 1.

[0036] Fig. 4 is a view which illustrates each of the functions of the digital camera represented in Fig. 1.

[0037] Fig. 5 is a block diagram which shows the inner structure of the digital camera represented in Fig. 1.

[0038] Fig. 6 is a block diagram which shows the details of the structure of the camera unit of the digital camera represented in Fig. 1.

[0039] Fig. 7 is a block diagram which shows the details of the PHS unit of the digital cameral represented in Fig. 1.

[0040] Fig. 8 is a flowchart which illustrates the program to perform the photographing operation of the digital camera represented in Fig. 1.

[0041] Fig. 9 is a flowchart which illustrates the program to execute the interruptive process by use of the corresponding keys for the photographing operation represented in Fig. 8.

[0042] Fig. 10 is a flowchart which illustrates the program to execute the play back function for the interruptive process represented in Fig. 9.

[0043] Fig. 11 is a flowchart which illustrates the program to execute the operation of the image reproduction (indication) for the digital camera represented in Fig. 1.

[0044] Fig. 12 is a flowchart which illustrates the program to execute the link establishment process of an electronic mail for the digital camera represented in Fig. 1.

[0045] Fig. 13 is a flowchart which illustrates the program to execute the transmission and reception processes for the electronic mail represented in Fig. 12.

[0046] Fig. 14 is a flowchart which illustrates the program to execute the transmission and reception processes for the electronic mail represented in Fig. 12.

[0047] Fig. 15 is a block diagram which conceptually shows the control flow of the digital camera represented in Fig. 1.

[0048] Fig. 16 is a flowchart which illustrates the program to execute the control of the amount of a photographing image for the digital camera represented in Fig. 1.

[0049] Fig. 17 is a block diagram which conceptually shows the control flow of the digital camera represented in Fig. 1 in accordance with a second embodiment of the present invention.

[0050] Fig. 18 is a flowchart which illustrates the program to execute the control of the amount of receiving data for the digital camera in accordance with the second embodiment of the present invention.

[0051] Fig. 19 is a flowchart which illustrates the program to execute the control of the amount of receiving data for the digital camera represented in Fig. 1 in accordance with a third embodiment of the present invention.

[0052] Fig. 20 is a flowchart which illustrates the program to execute the control of the amount of receiving data for the digital camera represented in Fig. 1 in accordance with a fourth embodiment of the present invention.

[0053] Fig. 21 is a flowchart which illustrates the program to execute the control of the amount of receiving data for the digital camera represented in Fig. 1 in accordance with a fifth embodiment of the present invention.

[0054] Fig. 22 is a flowchart which illustrates the program to execute the control of streaming data received by the digital camera represented in Fig. 1 in accordance with a sixth embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0055] Hereinafter, in conjunction with the accompanying drawings, the description will be made of the embodiments in accordance with the present invention.

(First Embodiment)

[0056] The image processing method of the present invention will be executed by a digital cameral shown in Fig. 1, for example.

[0057] The image processing apparatus or the image input device of the present invention is applicable to this digital camera 100.

[0058] Here, in accordance with the first embodiment, the digital camera 100 is provided with the communicating function, such as telephone, electronic mail, and as shown in Fig. 1 (which shows the outer appearance of the appa-

ratus), there are provided on the front of the digital camera 100, a shutter button 102, a mode dial 101, a lens 108, and a stroboscope 108 which is arranged above the lens 108.

[0059] Also, on the side end of the digital camera 100 main body, there are arranged a speaker 105, a black and white liquid crystal display 104, a key board 103, a jog dial (not shown) which will be described later, and a microphone 106 incorporated in the main body of the digital camera.

[0060] Further, on the surface opposite to the plane where the shutter button 102, the mode dial 101, the lens 108, and the stroboscope 109 are arranged, a pointing device 110 is provided as shown in Fig. 2 (which shows the outer appearance of the apparatus, observed in the direction indicated by an arrow A in Fig. 1).

[0061] Furthermore, as shown in Fig. 2, the portion where the speaker 105 is provided is arranged in such a manner that it is freely opened from or closed to the digital camera 100 main body in the direction indicated by an arrow B. The structure is arranged so that a color liquid crystal display 107 is made observable when this portion is open.

[0062] Here, the mode dial 101 is also provided with the power switching function, and as shown in Fig. 3 (the front view of the mode dial 101, observed in the direction indicated by an arrow C in Fig. 1), this dial is structured so as to be rotative around the shutter button 102.

[0063] Then, with the rotation of this mode dial 101, it is made possible to switch the modes in which the power-supply is turned off (OFF mode); the telephone is made ready for transmission and reception (TEL mode); the image, audio, text, and other information, which are stored in the main body of the digital camera 100, are indicated on the display (VIEW mode); and some more.

[0064] Here, Fig. 4 shows the respective functions of each of the modes of the digital camera 100 represented in Fig. 1.

[0065] As shown in Fig. 4, the telephone call can be received (the TEL called function is ready) in the modes other than the OFF mode.

[0066] In the TEL mode, the usual PHS (personal handy-phone system) telephone set becomes operative (that is, the TEL called and TEL calling functions are ready). In other words, it becomes possible to input a telephone number from the key board 103 on the digital camera 100 main body, to indicate the input number on the black and white LCD 104, and to indicate on it the telephone numbers stored in advance (the display of a personal telephone directory) in the TEL mode. Then, the transmission and reception of a telephone call are made by use of the speaker 105 and the microphone 105 incorporated in the digital camera 100 main body.

[0067] Also, in the TEL mode, indications are made possible on the color LCD 107 as required so as to select any one of the complicate optional functions easily by the application of color-coding or the like.

[0068] Here, the phrase "the transmission and reception of a telephone call" means to include the data communication that may be executable by use of the PHS telephone set, the portable telephone set, or the like.

[0069] In the VIEW mode, the arrangement is made to select either the image obtained by photographing in the CAMERA mode which will be described later, the recorded audio, the received image and audio, or the text, and then, to reproduce any one of them or to display it (that is, the image display/output function, audio output function, text display function, and electronic mailing function).

[0070] In the CAMERA mode, although the details will be described later, the photographing object via the lens 108 is photoelectrically converted into the electric signals by means of the CCD (charge coupled device) or some other photographing device, and stored on a flash memory or other storage device after given image processes are executed as required (that is, the image input/storage function).

[0071] Also, in the CAMERA mode, it is possible to select, by use of the pointing device 110, the condition of stroboscopic emission from among those on the menu shown on the color LCD 107, and to illuminate the object under the condition thus selected.

[0072] Further, in the CAMERA mode, it is possible to confirm the image obtained by photographing by use of the play back function which will be described later, and then, to erase it if unwanted or record the audio data as annotation (that is, the audio input/storage function), or to send it to the desired party as the electronic mail (the electronic mail function).

[0073] The inner structure of such digital camera 100 as described above is mainly arranged with the main CPU unit 201, the sub-CPU unit 202, the PHS unit 203, and the camera unit 204 as shown in Fig. 5, for example. With the cooperative operations of each of the units, it becomes possible for the TEL mode, the VIEW mode, and the CAMERA mode to execute each of the functions as given below.

[0074] Now, hereunder, the specific description will be made of the main CPU unit 201, the sub-CPU unit 202, the PHS unit 203, and the camera unit 204.

(1) Camera Unit 204

[0075] Fig. 6 is a diagram which specifically shows the camera unit 204 represented in Fig. 5.

[0076] As shown in Fig. 6, the camera unit 204 comprises the photographing device 213 where the incident light

Ex.1002 / Page 249 of 1385
APPLE INC.

from the lens 108 shown in Fig. 1 is focused into an image on the photographing plane; the CDS/AGC circuit 214 to which is supplied the output of the photographing device 213; the A/D converter 215 to which is supplied the output from the CDS/AGC circuit 214; the signal processing circuit (image processor) 216 to which is supplied the output of the A/D converter 215; and the camera microcomputer 211 which is connected with the CPU 29 (Fig. 5) of the main CPU unit 210 which will be described later in detail. The output from the camera microcomputer 211 is supplied to the image processor 216. Then, the output from the image processor 216 is supplied to the CPU 29.

[0077] Also, the camera unit 204 is provided with the timing generator 218 to which the output from the CPU 29 is supplied, and also, provided with the vertical driver 217 to the output from the timing generator 218 is supplied. The output from the timing generator 218 is supplied to each of the photographing device 213, the CDS/AGC circuit 214, the A/D converter 215, and the image processor 216. The output from the vertical driver 217 is supplied to the photographing device 213.

[0078] Further, the output from the CPU 29 is supplied to the image processor 216.

[0079] In the camera unit 204 thus arranged, the camera microcomputer 211 controls the entire operation of the camera unit 204 by communicating with the CPU 29 which controls the operation of the entire body of the apparatus. For example, the camera microcomputer 211 controls the operation of the respective image processes when receiving the information of the lens position of the lens 108 (Fig. 1), and transfers the information to the CPU 29 so as to prompt the user's operation in accordance with the aperture condition.

[0080] More specifically, at first, the lens 108 is a zoom lens of the three-time magnification, which is structured to shift the zooming positions manually, for example. In terms of a 35 mm camera, it has a focal length of 24 mm to 103 mm. Then, this lens position is given to the camera microcomputer 211 by means of hole device (not shown). Therefore, in accordance with given lens positions of the lens 108, the camera microcomputer 211 controls the operation of the camera unit 204 so as to perform various image processes.

[0081] Meanwhile, as to brightness, the lens is provided with the F2.4 to F3.5, and between the lens 108 and the photographing device 213, there are also provided two kinds of optical apertures, open and stop-down, although not shown in Fig. 6. These apertures are manually operated. Then, the camera microcomputer 211 detects the aperture positions to transfer the detected result to the CPU 29. Therefore, the CPU 29 is arranged to give warning or the like to the user when the amount of light is insufficient or excessive in accordance with the detected result of the camera microcomputer 211.

[0082] Also, the stroboscope 109 is provided with the lighting adjustment circuit. The charging and light emitting are also controlled by the camera microcomputer 211. In other words, the stroboscope 109 varies the reference level of the light adjusting control in accordance with the lens positions of the lens 108 (the zoom lens) provided by the camera microcomputer 211. Therefore, irrespective of the lens positions of the lens 108, it is made possible to obtain an appropriate light emission.

[0083] In this respect, the CPU 29 is, although described later in detail, formed by the IC of inclusive type having the memory controller and serial interface in it, which controls the operation of the entire body of the apparatus.

[0084] By the control made by the camera microcomputer 211 thus arranged, the camera unit 204 operates as given below.

[0085] At first, the clock K signal 230 generated by the CPU 29, which is the base of the timing of the apparatus entire body, and the horizontally and vertically synchronized signals 40 are supplied to the timing generator (TG) 218 at the display timing of the photographing device 108.

[0086] The timing generator 218 generates the timing signals at which to form images on the photographing device 213. In synchronism with the clock K signal 230 and the horizontally and vertically synchronized signals 40 from the CPU 29, the timing generator supplies the timing signal 226 (which is the basic timing signal for the image formation) to the photographing device 213; the timing signal 227 (which needs the voltage conversion given to the photographing device 213) to the vertical driver 217; the sample hold signal 231 (which is the timing signal of the sample holding) to the CDS/AGC circuit 214; and the sample clock 228 (which is the basic clock at which to sample the image signals) to the A/D converter 215 and the image processor 216, respectively.

[0087] At this time, the lens 108 converges light on the photographing plane (charged surface) of the photographing device 213 by refracting light from the object (which is not shown) to be photographed.

[0088] The photographing device 213 is formed by CCD, for example, and the size of the image formed by the photographing device 213 is 1,280 horizontal pixels (dots) and 960 vertical pixels.

[0089] Then, the photographing device 213 converts the light from the object on the lens 108 into electric signals (charges) in accordance with the timing signal 226 from the timing generator 218, and supplies the electric signals thus converted to the CDS/AGC circuit 214 as analogue image signals 222.

[0090] Also, the vertical driver (V-Driver) 217 converts the voltage amplitude of the signal that drives the photographing device 213 in accordance with the timing signals 227 from the timing generator 218.

[0091] In this way, the electric signals having the 1,280 horizontal pixels and 960 vertical pixels are supplied to the CDS/AGC circuit 214 as signals of the photographed image.

Ex.1002 / Page 250 of 1385
APPLE INC.

[0092] In accordance with the sample hold signals 231 from the timing generator 218, the CDS/AGC circuit 214 performs the sampling process and removes noises from the photographed image signals 222 from the photographing device 108. Also, the gain of the signal amplitude is automatically controlled. Then, the CDS/AGC circuit 214 supplies the photographed image signals 223 thus processed to the A/D converter 215.

[0093] The A/D converter 215 converts the photographed image signals (analogue pixel signals) from the CDS/AGC circuit 214 into the 10-bit digital data 64 in accordance with the sample clock 228 from the timing generator 218, and supplies the digital data 224 to the image processor 216 via the 10-data bus.

[0094] The image processor (signal processing circuit) 216 is an image processing IC. Then, the control signals 221 from the CPU 29 are given to the image processor 216 through the camera microcomputer 211. Therefore, the image processor 216 executes the image processes, such as the white balancing, the AE and more by reading from or writing to the inner registers (not shown) in accordance with the control signals 221.

[0095] More specifically, the image processor 216 performs the correction process, such as the white balancing, for the digital data from the A/D converter 215 in accordance with the sample clock 228 from the timing generator 218. Then, the image processor converts such data from the color space available at the photographing device 213 to the color space of the RGB system, and then, makes them the image data 39 in the YUV 8-bit format to be supplied to the CPU 29 through the 8-data bus.

(2) Sub-CPU Unit 202

[0096] As shown in Fig. 5, the sub-CPU unit 202 is provided with the sub-CPU 1 which communities with the main CPU unit 201, the PHS unit 203, and the camera unit 204 described above. With the sub-CPU 1, there are connected the black and white LCD display 104, the jog dial 11, the key board 103, the mode dial 101, the shutter button 102, the RTC 4, the DC-DC converter 24, and the battery 22.

[0097] The sub-CPU unit 202 thus arranged has the functions given below.

(2-1)

[0098] The sub-CPU 1 exchanges the commands and data by communicating with the CPU 29 of the main CPU unit 201.

[0099] As means for this communication, the parallel transfer is performed by use of the bus 19 formed by 13 signals lines. The bus 19 comprises an 8-data bus, a one-address signal line, an I/O READ line, an I/O WRITE line, a chip selection line, and an INTERRUPT signal line.

[0100] Also, the sub CPU 1 supplies the reset request signal Reset of the main CPU unit 201 to the CPU 29 through the signal line 20.

[0101] Further, the sub-CPU 1 supplies the rest request signal Rest of the camera unit 204 control to the camera microcomputer 51 through the signal line 21.

(2-2)

[0102] The sub-CPU 1 communicates with the PHS module 48 of the PHS unit 203 to exchange commands, data, and some more between them.

[0103] As this communication means, the serial transfer is performed using the signal line 16 for serial data carrier signals (TxD and RxD), the signal line 17 for RING signals, and the signal line 18 for WakeUp signals.

[0104] Also, the sub-CPU 1 supplies the rest request signal Reset to the PHS module 48 of the PHS unit 203 through the signal line 18.

(2-3)

[0105] The sub-CPU 1 controls the display operation of the black and white LCD 104 by serially transferring the commands, data, and the like through the signal line 3 for use of the CS signal, RS signal, SDA signal, and SCL signal in order to allow the black and white LCD 104 to display telephone numbers and others.

[0106] Also, the sub-CPU 1 controls the ON/OFF of the back light (not shown) of the black and white LCD 104 by supplying the BL-ON signal to the black and white LCD 104 through the signal line 3.

(2-4)

[0107] The sub-CPU 1 is connected with the RTC 4 through the I2C-BUS (Inter IC BUS: advocated by Philips Inc.).

[0108] The RTC 4 generates calendar, time, and other information. Also, the RTC 4 operates with the operation clock

Ex.1002 / Page 251 of 1385
APPLE INC.

of 32.768 kHz, and this operation clock is supplied to the PHS module 48 through the signal line 49.

[0109] It is arranged for the sub-CPU 1 to obtain the information of data, time, and some others by use of the RTC 4.

[0110] Also, the alarm signal is transmitted from the RTC 4 to the interruption terminal IRQ of the sub-CPU 1 through the signal line 6. In this way, the sub-CPU 1 is ready to operate interruption process at the time set in advance.

(2-5)

[0111] The sub-CPU 1 detects an input made by the key operation of the mode dial 101, the shutter button 102, the key board 103, or the like.

[0112] In other words, the sub-CPU 1 is arranged to be able to discriminate four modes: by detecting the current operational status of the mode dial 101 (mode change switch), the sub-CPU discriminates the OFF mode (the source-supply cut off mode), the TEL mode (the telephone mode), the VIEW mode (the reproduction mode), and the CAMERA mode (the camera mode) from one another. To this end, the sub-CPU 1 is connected with the mode dial 101 by four signal lines (switch input terminals) 8.

[0113] Also, the sub-CPU 1 detects the operational status of the shutter button 102 (the shutter switch). The shutter button 102 is a two-staged switch which enables the button to be in the state of being half depressed and completely depressed, respectively. Therefore, the sub-CPU 1 is arranged to determine whether the shutter button 102 is half depressed or completely depressed. To this end, the sub-CPU 1 and the shutter button 102 are connected by two signal lines (switch input terminals) 10.

[0114] Also, the sub-CPU 1 detects the operational status of the jog dial 11.

[0115] The jog dial 11 is used for selecting the target item of a plurality of items indicated on the screen of the black and white LCD 104. For example, the user rotates the jog dial 11 to move the cursor on the screen of the black and white LCD 104. When the cursor is positioned on the target item, the item is determined by depressing the jog dial 11. Also, the jog dial 11 is composed so as to be capable of being switched over on the screen of the black and white LCD 104. For example, if the jog dial is inclined to the left, the screen returns to the previous indication. If it is inclined to the right, the screen is allowed to proceed to the next indication.

[0116] Such operational control accompanied by the operation of the jog dial 11 is performed by the sub-CPU 1 with its detection of the current operational status of the jog dial 11. Therefore, the sub-CPU 1 is connected with the jog dial 11 by a total of five lines (switch input terminals) 12, that is, two signal lines for use of discriminating two rotational directions; one signal line for use of discriminating the depression of the jog dial; and two signal lines for use of discriminating the left and right inclinations thereof.

[0117] Also, the sub-CPU 1 detects the operational status of the key board 103.

[0118] The key board 103 is used for inputting the telephone numbers. It is formed by switches of 8 x 2 key matrix type.

[0119] Therefore, the key board 103 is scanned by the sub-CPU 1 by use of the eight output signal lines (output terminals) 14 and two input signal lines (input terminals) 15.

[0120] Each of the keys, such as the mode dial 101, the shutter button 102, and the key board 103, among some others, is provided with a special input terminal which is used for interruption when any of the inputs should change. Therefore, when the sub-CPU 1 is on standby without any particular job to be executed, the sub-CPU 1 is allowed to shift from the standby status to the full-on status automatically if the key input changes, and then, execute the control processes to be made following such changes of input.

(2-6)

[0121] The sub-CPU 1 is connected with the battery 22 through the signal line 26. Then, by the signal line 26, serial communications are carried out by use of the RxD. For example, the sub-CPU 1 receives the remaining amount of the cell energy from the battery 22 or information on the battery when it has been charged (voltage, temperature, and some more), and performs the control processes in accordance with the information thus received.

[0122] Here, the electric power of the battery 22 is given to each section of the sub-CPU unit 202 through the DC-DC converter 24. Then, the sub-CPU 1 conducts the power management by controlling the ON/OFF of the DC-DC converter 24 through the signal line (output terminal) 25.

[0123] Also, the battery 22 is provided with the attachment/detachment detection switch 23 which is interlocked with the knob (not shown) of the lid of the outlet opening for the battery 22. The detection signals of the attachment/detachment detection switch 23 is supplied to the sub-CPU 1 through the communication line 27. The sub-CPU 1 is arranged to sense the status where the battery 22 is about to be withdrawn by the detection signal emitted from the attachment/detachment detection switch 23, and to carry out the power off process at that time. In this way, it is arranged to prevent data and others on the memory from being destroyed.

[0124] Further, the output voltage of the battery 22 is supplied to the sub-CPU 1 through the signal line (A/D converter input terminal) 28. Then, the sub-CPU 1 monitors the voltage of the battery 22. If any excessive charging, excessive

Ex.1002 / Page 252 of 1385
APPLE INC.

discharging, or any other abnormal condition is detected, the corresponding protection processes are effectuated accordingly.

(3) PHS Unit 203

[0125] Fig. 7 shows specifically the inner structure of the PHS unit 203, for example.

[0126] In other words, as shown in Fig. 7, the PHS unit 203 comprises the antenna switch 252 which is connected with the antenna 251; the reception amplifier (AMP) 265 to which is supplied the output of the antenna switch 252; the synthesizer 257; the reception circuit 254 to which is supplied each of the outputs of the reception amplifier 265 and the synthesizer 257; the ADPCM codec circuit 260, the PIAFS frame disassemble/assemble circuit 262, and the control circuit 263, to which the output of the TDMA deframer circuit 259 is supplied, respectively; and the application unit (hereinafter referred to as application) 264 which is connected with the control circuit 263. The PIAFS frame disassemble/ assemble circuit 262 is connected with the control circuit 263, and also, with the application 264. The synthesizer 257 is arranged so that the output of the control circuit 263 is supplied to it. Also, the speaker and receiver set 261 is connected with the ADPCM codec circuit 260.

[0127] Also, the PHS unit 203 comprises the TDMA framer circuit 258 to which is supplied each of the outputs of the control circuit 263 and the ADPCM codec circuit 260; the transmission circuit 255 to which is supplied each of the outputs of the synthesizer 257 and the TDMA framer circuit 258; and the transmission amplifier 253 to which is supplied each of the outputs of the control circuit 263 and the transmission circuit 255. The output of the transmission amplifier 253 is sent out from the antenna 251 by way of the antenna switch 252.

[0128] With the PHS unit 203 as described above, the operation is performed to switch, at first, the antenna switch 252 so that the transmission path that sends out data from the antenna 251 is switched over to the reception path that receives data from the antenna 251, and vice versa.

[0129] The control circuit 263 makes the control of each of the functional blocks (each of the circuits), and at the same time, accepts the requests from the application 264, and also, notifies each status to the application 264.

[0130] The application 264 is formed by the application of each of the functions that perform the corresponding service. For example, the application operates in response to the operation of the sub-CPU 1 of the sub-CPU unit 202, the CPU 29 of the main CPU unit 201, and each of the softwares (each of the programs to be described later). Then, to the PHS unit 203, the sub-CPU 1 gives each command and data related to the operation of the PHS unit. The communications carried out by the PHS unit 203 are controlled by the CPU 29.

[0131] Now, when transmission is made, the antenna switch 252 is, at first, switched over to the reception path.

[0132] Then, in accordance the control of the control circuit 263, the PIAFS frame disassemble/assemble circuit 262 processes the assembling process for the data provided by the application 264 for transmission on the basis of the PHS data communication regulation (PIAFS standard). After that, the PIAFS frame disassemble/assemble circuit 262 supplies the transmission data thus assembled to the TDMA framer circuit 258.

[0133] At this juncture, the message information TX_MSG is also supplied from the control circuit 263 to the TDMA framer circuit 258.

[0134] Also, the ADPCM codec circuit 260 digitizes the audio data inputted from the speaker and receiver set 261, and supplies it to the TDMA framer circuit 258.

[0135] Therefore, the TDMA framer circuit 258 assembles on the communication framer (TDMA frame) the message information TX_MSG from the control circuit 263 and the data TCH_TX from the PIAFS frame disassemble/assemble circuit 262 and the ADPCM codec circuit 260, and supplies the assembled data to the transmission circuit 255.

[0136] Here, the control circuit 263 transmits to the synthesizer 257 the standard signal of a certain frequency to designate a carrier. In this way, the synthesizer 257 designates the carrier of the transmission circuit 255.

[0137] With the carrier thus designated by the synthesizer 257, the transmission circuit 255 modulates the data from the TDMA framer circuit 258, and supplies them to the transmission amplifier 253.

[0138] The transmission amplifier 253 amplifies the data from the transmission circuit 255 in accordance with the control (TX_POWER) of the control circuit 263, and transmits them from the antenna 251 through the antenna switch 252.

[0139] At the reception, on the other hand, the antenna switch 252 switches over the current path to the reception path at first.

[0140] Then, the data are received from the antenna 251 and amplified by the reception amplifier 265. After that, the data thus amplified are supplied to the reception circuit 254.

[0141] At this juncture, the control circuit 263 designates a carrier by transmitting the standard signal of a certain frequency. In this way, the synthesizer 257 designates the carrier for the reception circuit 254.

[0142] With the carrier thus designated by the synthesizer 257, the reception circuit 254 demodulates the reception data from the reception amplifier 265, and supplies them to the TDMA deframer circuit 259.

[0143] The TDMA deframer circuit 259 disassembles the reception data (data frame) from the reception circuit 254

Ex.1002 / Page 253 of 1385
APPLE INC.

into the message information RX_MSG to the control circuit 263, and the information data on communication TCH_RX, such as audio and PIAFS data, and then, supplies the message information RX_MSG to the control circuit 263, and the information data on communication TCH_RX to the ADPCM codec circuit 260 and to the PIAFS frame disassemble/assemble circuit 262, respectively.

[0144] The ADPCM codec circuit 260 converts the audio data contained in the information data on communication TCH_RX from the TDMA deframer circuit 259 into the analogue data, and outputs them to the speaker and receiver set 261 as voices.

[0145] In accordance with the control of the control circuit 263, the PIAFS frame disassemble/assemble circuit 262 performs the disassembling process of the information data on communication TCH_RX from the TDMA deframer circuit 259 on the basis of the PHS communication regulation (PIAFS standard). Then, the PIAFS frame disassemble/assemble circuit 262 supplies the data obtained by such disassembling to the application 264.

[0146] The control circuit 263 supplies the message information RX_MSG from the TDMA deframer circuit 259 to the application 264.

[0147] The application 264 performs the respective processes for the data from the PIAFS frame disassemble/assemble circuit 262 and the control circuit 263.

(4) Main CPU Unit 201

[0148] As shown in Fig. 5, the main CPU unit 201 comprises the aforesaid CPU 29; the EDODRAM 30 which is connected with the CPU 29; the flash ROM 31 and ROM 32; and the IrDALED 36 with which the IrDA module 35 and IrDA module 35 are connected.

[0149] Also, the main CPU unit 201 is provided with the crystal oscillators 46 and 47 installed for the CPU 29.

[0150] For the main CPU unit 201 thus arranged, the CPU 29 (the CPU chip) is at first provided with three serial ports (SerialPorts 0 to 2).

[0151] The signal line 38 of the serial port SerialPort 0 is used for communication with the camera unit 204. Therefore, the CPU 29 issues instructions to the camera regarding the exposure condition, the use of stroboscope, the photographing modes and timing, and others through this signal line 38.

[0152] The signal line 37 of the serial port SerialPort 1 performs the IrDA communication with the external host computer (not shown). Here, the IrDA module 35 converts the serial data provided through the signal line 37 into the data for use of IrDA, and then, performs the infrared communication of the data obtained by the IrDA module for use of the IrDA by means of the IrDALED 36 (driver/receiver).

[0153] The signal line 34 of the serial port SerialPort 2 is used for communication with the wireless communication unit (not shown). To the wireless communication unit, commands are issued from the sub-CPU 1 of the sub-CPU unit 202, while the communication data are provided by the CPU 29 through the signal line 34. Therefore, it becomes possible to collect instructions and information to the wireless communication unit without interrupting the transmission while the wireless communication is being made. This communication is usable to obtain the information of the field intensity, for example.

[0154] Also, the CPU 29 is provided with the parallel interface 19, and the sub-CPU unit 202 and the main CPU unit 201 are connected by use of this parallel interface 19.

[0155] Further, the CPU 29 executes the image capturing; the interpolation and thinning processes of image signals; display outputs to the black and white LCD 104 and the color LCD 107; communications with the camera microcomputer 211 of the camera unit 204, and with the sub-CPU 202, as well as with the aforesaid wireless communication unit; communications with the external host computer; the protocol processes usually used for the inter net, such as TCP/IP; and the user's application such as electronic mails or WWW.

[0156] Therefore, the CPU 29 comprises the interface 39 and display interface 41 of the camera unit 204, besides, although not shown, it comprises serial ports, memory interface, parallel interface, general purpose I/O (hereinafter referred to as GPIO), arithmetic unit, cache storage, DMA controller, timer, and compression and expansion engines, among some others.

[0157] In this respect, the interface 39 of the camera unit 204 and the display interface 41 will be described later in detail.

[0158] It is also made possible to call interruption with respect to the interface of the camera unit 204, the display interface, the timer, and DMA controller, the GPIO, the serial interface, the parallel interface, and the compression and expansion engines when each of the respective operations should be changed or some other event should take place.

[0159] For the DMA channel, it is arranged to be able to perform the data transfer as soon as data are ready without any intervention of the arithmetic unit, because the interface of the camera unit 204, the display interface, the serial interface, and the compression and expansion engines are allocated to this channel.

[0160] The EDODRAM 30 is used as the working area of the OS and the application software. Here, the EDODRAM 30 is formed by two EDODRAMs each having 16 M (1 x 16) bit at 3.3 V.

Ex.1002 / Page 254 of 1385
APPLE INC.

[0161] Here, the EDODRAM 30 supports the self refresh mode, and it is arranged to be shiftable to the low power dissipation status by the control of the memory controller (not shown) of the CPU 29.

[0162] The flash ROM 31 is the NOR type memory, for example, which is connected in the same mode as the usual SRAM when serving as a hardware interface.

[0163] The flash ROM 31 is used for storing images obtained by the photography performed in the camera unit 204, and for recording received electronic mails, data obtained by the ftp communications, audio data from the speaker and receiver set 261 (microphone) of the PHS unit 203, and various data such as parameters.

[0164] Then, writing to the flash ROM 31 is made in accordance with the protocol of the software program to be executed on the CPU 29.

[0165] The ROM 32 is formed by the 16M-bit mask ROM, for example, and stores the OS and the programs of the application software themselves.

[0166] This ROM 32 is selected when the power-supply is turned on for the CPU 29 or after the release of resetting. Then, the bootstrap code is selected.

[0167] The crystal oscillators 46 and 47 generate the frequency to be used in the CPU 29.

[0168] The crystal oscillator 46 generates the frequency to be used when the entire system is controlled and the NTSC is coded. On the other hand, the oscillator 47 generates the frequency to be used when data are obtained from the camera unit 204 (for data input)

[0169] These crystal oscillators 46 and 47 are structured so as to suspend its oscillations in the circumstance of the low power consumption.

[0170] The interface 39 of the camera unit 204 is used when the image data transferred from the camera unit 204 are stored on the flash ROM 31.

[0171] Here, the image data thus transferred are the data in the format of 4:2:2 of the image signals (CCDRaw data) obtained by the photography using the photographing device 213 after the image is processed in the image processor 216 as to the color space conversion, image interpolation, automatic exposure adjustment, automatic white balancing, automatic focusing, and so on. As a result, there is a need for the generation of the sampling frequency which is two times the usual CCDRaw data.

[0172] Here, the CPU 29 provides the horizontally synchronized signal HD and vertically synchronized signal VD for the image processor 216 and the timing generator 218 of the camera unit 204 through the signal line 40. In this way, it becomes possible to store the image data on the flash ROM at the timing in synchronism with the camera unit 204.

[0173] The display interface 41 is used for providing the output NTSC signals from the CPU 29 for the external connector 42 and the LCD controller 53 of the color LCD 107 as well.

[0174] Therefore, the LCD controller 45 supplies the NTSC signals obtained from the display interface 41 to the color LCD 43 through the voltage conversion device 44.

[0175] These have been the descriptions of the main CPU unit 210, the sub-CPU unit 220, the PHS unit 230, and the camera unit 240, which form the principal structure of the digital camera 100.

[0176] Now, the specific description will be made of the operational control when the digital camera 100 is used for photographing.

(1) The Control of the Photographing Operation in the CAMERA Mode

[0177] On the ROM 32, a program is stored in advance in accordance with the flowchart shown in Fig. 8, for example. When this program is read by the CPU 29 for execution, the photographing operation is carried out by the digital camera 100 as given below.

[0178] In other words, when the power-supply is turned on by operating the mode dial 101 of the digital camera 100 or the CAMERA mode is switched on at first (step S501), charging begins to charge the capacitor for use of stroboscopic emission (step S502). This is because the stroboscopic emission should be ready for immediate use when the stroboscopic photographing mode is further dialed in the CAMERA mode.

[0179] Then, the operation of the camera microcomputer 211 (the CCD module that includes the controller) is enabled (step S503) to control the photographing device 213 and the like in the camera unit 204. Continuously, then, the operation begins so as to make the color LCD 107 functional as an electronic view finder (EVF) for the confirmation of an object (not shown) to be photographed (step S504).

[0180] Now, when the photographing begins, the continuous processes from the image that has been taken in the camera unit 204 up to the display thereof on the screen of the color LCD 107 are carried out in the following steps:

[0181] At first, the optical information of the object that has been taken in from the lens 108 is converted into the electric signal by use of the photographing device 213 (photoelectric conversion process) (step S505).

[0182] The output signal of the photographing device 213 is the interlace analogue signal. Then, in order to make the processing speed faster, it is arranged to compress data to a size of 320 x 320 pixels by the application of thinning process, not the data having the total pixels of 1,280 x 960.

Ex.1002 / Page 255 of 1385
APPLE INC.

[0183] Subsequently, the signal obtained in the step S505 is transmitted to the image processor 216 for the execution of the image process described above (step S506). In other words, the correction processes, such as the automatic white balancing, AE, and stroboscopic photography, are executed. The image process, such as conversion to the YCrCb (4:2:2) format, is also executed in this step.

[0184] Here, the signal obtained in the step S506 (that is, the signal converted into the YCrCb format) is further processed by the application of a software in order to correct the deviation in the aspect ratio resulting from the difference in the output image signal on the color LCD 107 (EVF) and the processing frequency (step S507).

[0185] Then, the signal processed in the step S506 and step S507 is converted into the NTSC signal by use of the NTSC encoder (not shown) (step S508). The signal thus processed is supplied to the LCD controller 45 of the color LCD 107 (step S509).

[0186] Consequently, the image of the object observed by the EVF is indicated on the screen of the color LCD 107 by the signal output of the LCD controller 45 (step S510).

[0187] Each of the processing steps S505 to step S510 as described above is executed as a continuous loop at a cycle of 1/30 second. Thus, the objective image is always monitored on the screen of the color LCD 107.

[0188] Now, during the monitoring period on the color LCD 107, if the photographer operates any one of the keys, an interruption event takes place following the detection signal thereof. Then, the process shifts to the interruption process A.

(1-1) Interruption Process A

[0189] On the ROM 32, a program is stored in advance in accordance with the flowchart shown in Fig. 9. When this program is read by the CPU 29 for execution, the interruption process is enabled (the interruption process by the key operation) for its execution as given below.

[0190] Here, in the stage where the key operation is made, either one of the two modes is internally designated. One of them is the normal mode, which is the mode as shown in Fig. 8 wherein the monitoring operation of a photographed image is continuously performed since the power-supply has been turned on. The other one is the half depressed mode where the shutter button 102 is half depressed once to lock each of the camera settings, and then, in such status, the monitoring operation of the image takes place.

[0191] Here, now, these processes are divided into two, and the description will be made of the starting position of the processes by the one to be carried out in the normal mode, and the other to be carried out beginning with the half depressed mode.

(1-1-1) The Interruption Process in the Normal Mode

[0192] At first, the key status is read (step S521) to detect which one of the keys is operated.

[0193] Then, in accordance with the key status fetched in to the step S521, the current setting values are locked (step S523) with respect to the various camera settings in the image processor 216, such as the automatic white balancing, AE, stroboscopic correction in case of a stroboscope 109 photography, if it is determined that the shutter switch 102 has been operated (step S522). Then, the operation of the color LCD 107 (EVF) is suspended (step S537) in order to reduce the processing load on the CPU 29.

[0194] Subsequently, the capture signal is fetched in for the full image of 1,280 x 960 pixels as the photographed image, although, as described earlier, the monitoring image process has been made only for the signal having the pixel numbers of a compressed image size for the purpose of speeding up the required processes. Then, after given image processes have been executed in the image processor 216, the data is stored in the EDODRAM 30 in the YCrCb format (step S538).

[0195] The data thus stored in the EDODRAM 30 in the step S538, the image depression process is carried out (step S539) on the basis of the JPEG regulation. The compressed data are written on the flash ROM 31 as an image file (step S540).

[0196] Then, the color LCD 107 whose operation has been suspended is restored (step S541), and the image file written on the flash ROM 31 is displayed on the screen of the color LCD 107 for a given period of time (step S542) so that the confirmation of the photographed image is made possible. Thus, the current interruption process is completed (step S543). The process returns to the loop process shown in Fig. 8 to resume the monitoring process of the image.

[0197] On the other hand, if it is determined that the Play back key is operated by the key status fetched in to the step S521 (step S524), the process of the Play back function will be executed as described later.

[0198] Also, if it is determined that the shutter button 102 has been half depressed by the key status fetched in to the step S521 (step S525), the inner state of setting is defined to be the half depressed mode (step S526). Then, as in the step S523 described above, each of the camera settings in the image processor 216, such as the automatic white balancing, AE, stroboscopic correction in case of a stroboscope photography, is locked at the current setting

Ex.1002 / Page 256 of 1385
APPLE INC.

value, respectively (step S527).

[0199] After that, the current interruption process is completed (step S528). The process will return to the loop process as shown in Fig. 8. Then, the monitoring process of the image is resumed.

[0200] Also, if it is determined that the key operation has been made to change the photographing conditions by the key status fetched in to the step S521 (step S529), the inner state of each setting in the image processor 216, such as the automatic white balancing, AE, stroboscopic correction in case of a stroboscope photography, is modified to be set again at the designated conditions (step S530). Then, the current interruption process is completed (step S528). The process will return to the loop process as shown in Fig. 8. Then, the monitoring process of the image is resumed.

[0201] Also, if it is determined that the OFF key (source-supply off) is operated by the key status fetched in to the step S421 (step S531), the operation of the color LCD 107 is terminated (step S532). The operation of the CCD module is also terminated (step S533) one after another. Then, after the other photographing operations are terminated, the source-supply process is turned off (step S534).

[0202] On the other hand, if it is not determined in the step S531 that the OFF key (source-supply off) is operated, it is interpreted that no effective key operation has been made. The current interruption process is then terminated (step S528) without executing any processes. The process will return to the loop process as shown in Fig. 8, and the image monitoring process is resumed.

(1-1-2) The Interruption Process in the Half Depressed Mode

[0203] At first, the key status is read in order to detect which one of the keys is operated (step S535).

[0204] If it is determined that the shutter switch 102 is operated by the key status fetched in to the step S521 (step S536), the processes beginning with the step S537 described above are executed, while each of the camera settings in the image processor 216 which has been locked (step S527) by the previous detection of the half depressed key (step S525) is still kept effective.

[0205] On the other hand, if it is determined that the half depression of the shutter switch 102 has been released by the key status fetched in to the step S521 (step S545), the inner status settings in the half depressed mode are released (step S546). Then, the current interruption process is terminated (step S528). The process will return to the loop process as shown in Fig. 8, and the monitoring of the image is resumed.

[0206] Also, if it is not determined that the half depression of the shutter switch 102 has been released by the key status fetched in to the step S521 (step S545), it is interpreted that no effective key operation has been made. The current interruption process is then terminated (step S528) without executing any processes. The process will again return to the loop process as shown in Fig. 8, and the image monitoring process is resumed.

(1-2) The Process of the Play Back Function B

[0207] The process of the Play back function B is executed when it is determined in the key operation determination process (step S524) in Fig. 9 that the key is operated to function the Play back.

[0208] Here, the Play back function is to make it possible to effectuate action upon an image immediately after having been photographed, such as the provision of audio information or the like (the function of audio addition), the transfer of image information by use of the electronic mail (the mail transfer function), the deletion of images (the image delete function), among some others, by means of simple key operations without changing modes.

[0209] Now, therefore, the ROM 32 is provided in advance with a stored program in accordance with the flowchart shown in Fig. 10. When this program is read by the CPU 29 for execution, the processes of the Play back function will be made as given below.

[0210] At first, it is determined whether or not there is any image that has been obtained by photographing immediately before (step S551).

[0211] The image taken immediately before means a photographed image which has been kept effective since the photographing operation has been executed by use of the shutter button 102 up to the moment the mode is changed or any one of other functional operations is performed.

[0212] Then, if it is found as a result of the detection that there is no image taken immediately before, no process will be executed, and the current interruption process is terminated (S540). The process will return again to the loop process as shown in Fig. 8. The image monitoring is resumed.

[0213] On the other hand, if there is any image that has been taken immediately before, the correction process is executed, at first, by the application of software with respect to the aspect ratio resulting from the difference in processing frequency for such image taken immediately before as has been written on the EDODRAM 30 in the same manner as the processes executed in the step S507 to the step S510 as shown in Fig. 8 (step S552).

[0214] Then, the signal processed in the step S552 is converted into the NTSC signal (step S553) by use of the NTSC encoder (not shown). The signal thus converted is supplied to the LCD controller 45 of the color LCD 107 (step

Ex.1002 / Page 257 of 1385
APPLE INC.

S554).

[0215] Consequently, the object image is displayed on the screen of the color LCD 107 by means of the EVF (step S555) with the output signal of the LCD controller 45.

[0216] After that, the kind of the Play back functions which has been selected by the photographer is distinguished (step S556). Then, the process is branched out to the corresponding one accordingly.

[0217] In other words, if the audio addition function is selected, the audio addition process will be executed (step S557). If the mail transfer function is selected, the mail transfer process will be executed (step S558). If the image deleting function is selected, the corresponding process will be executed to delete the photographed image (step S559).

(2) VIEW Mode (Image Display Mode)

[0218] The View mode is to reproduce (display) the image that has been obtained by photographing.

[0219] Here, therefore, a program is stored on the ROM 32 in accordance with the flowchart shown in Fig. 11. When the program is read by the CPU 29 for execution, the operation of the VIEW mode of the digital camera 100 will be carried out as given below.

[0220] At first, the source-supply is turned on by the operation of the mode dial 101 of the digital camera 100 or the VIEW mode is dialed to be switched (step S571), the operation of the color LCD 107 begins (step S572) so that the color LCD 107 operates as the electronic view finder (EVF) for the confirmation of an object when it is photographed.

[0221] Now, as shown in Fig. 9, the compressed image file, which has been written on the flash ROM 31 by the writing process of the photographed image (step S540) is read (step S573). Then, the decompression process, that is, the process to convert the compressed data on the basis of the JPEG standard into the original data (the data in the YCrCb format), is executed (step S574).

[0222] After that, the original data thus obtained by decompression in the step S574 is written on the EDODRAM 3 (step S575).

[0223] Thereafter, in the same manner as the processes in the step S507 to the step S510 shown in Fig. 8, the correction process and others will be executed (step S576) by the application of software as to the deviation of the aspect ratio resulting from the difference in the processing frequency for the original data (image data) written on the EDODRAM 30. Then, by use of the NTSC encoder (not shown), the data is converted into the NTSC signal (step S577), and supplied to the LCD controller 45 of the color LCD 107 (step S578).

[0224] Therefore, on the color LCD 107, the selected image by the designation of the EVF is displayed on its screen by use of the output signal of the LCD controller 45 (step S579).

(3) The Operational Control of the Electronic Mail at the Time of Transmission and Reception

[0225] A program is stored on the ROM 32 in accordance with the flowchart shown in Fig. 12 to Fig. 14, for example. When the program is read by the CPU 29 for execution, the transmitting and receiving operation of the electronic mail will be carried out for the digital cameral 100 as given below.

(3-1) The Link Establishment

[0226] Here, for example, it is assumed that the TCP/IP link establishment is made by the PPP (point to point protocol) using the telephone line.

[0227] In other words, as shown in Fig. 12, the connecting process for the telephone line begins, at first, by means of the AT command (step S581).

[0228] Then, it is determined whether or not the connection of the telephone line has been established (step S582), and if connected, the TCP/IP connection process begins by the PPP (step S583).

[0229] Subsequently, by the LCP (link control protocol), the link establishment process is executed for the data link layer (step S584).

[0230] Then, it is determined whether or not the user approval is needed (step S585). If needed, the protocol of the user approval will be executed (step S586).

[0231] If the user approval is not needed, the setting by the NCP (network control protocol) is confirmed (step S587). This confirmation should also be made after the execution of the user approval protocol when the user approval is needed.

[0232] Then, the connection by the PPP is established (step S588), and also, the connection by the LCP is established (step S589). After that, the current process is terminated.

Ex.1002 / Page 258 of 1385
APPLE INC.

(3-2) The Transmission of the Electronic Mail

[0233] If, for example, an electronic mail should be transmitted by the SMTP (simple mail transfer protocol), the SMTP client (hereinafter, simply referred to as a client) issues, at first, the request of connection to the SMTP server (hereinafter, simply referred to as a server) for the transmission and reception of an electronic mail (step S591).

[0234] When the server is connected by this request, the server returns to the client his response code indicating "connection OK".

[0235] When the client recognizes the reception of this response code (step S592), he declares to the server the commencement of use by notifying the server of his domain name by means of the HELO command (step S593).

[0236] Then, the server returns to the client the response code indicating "normal", together with the domain name of the server when the server recognizes the domain name of the client.

[0237] When the client recognizes the reception of this response code and the domain name of the server (step S594), he notifies the server of the From information by means of the MAIL command and declares the commencement of electronic mail transmission (step S595) by designating the user name (address) at the source of transmission.

[0238] Then, the server returns to the client the response code indicating "normal" when he recognizes that the user name (address) at the source of transmission is correct, and that the reception of this mail is ready by the reception of the From information from the client and the user name at the source of transmission.

[0239] When the client recognizes the reception of this response code (step S596), he designates the address of the mail for the server (step S597) by means of the RCPT command.

[0240] Here, if the mail should be sent to a plurality of parties, the plural mail addresses are designated in the step S597 accordingly.

[0241] Then, the server determines whether or not the mail address designated by the client is acceptable, and returns to the client the response code indicating "normal" if he can handle the address thus designated. If he cannot handle it, he returns the code indicating that the mail will be transferred to the other SMTP server.

[0242] When the client recognizes the reception of the normal response code (step S598), he declares to the server the text transmission of his mail by means of the DATA command (step S599).

[0243] If the reception is ready, the server returns to the client the response code indicating "the admission of the mail transmission" (the response code 354) when he receives from the client the declaration of the text transmission of his mail.

[0244] When the client recognizes the reception of this response code (step S600), he transmits to the server the text of his mail (step S601). Then, the client transmits the code indicated by <CR> <LF> <CR> <LF>, and the like to declare the finish of his text transmission (step S602). Here, in accordance with the present embodiment, it may be possible for the client to attach the image file, which is the file of photographed images, for example, or the file of received images to the text of his mail.

[0245] Then, the server returns to the client the response code indicating that he has completely complied with the client's request normally (the response code 250) when he receives the client's declaration of the termination of his text transmission.

[0246] When the client recognizes the reception of this response code (step S603), he declares to the server the termination of his transmission of the SMTP electronic mail (step S604).

[0247] Then, the server returns to the client the response code indicating "termination" when he receives the client's declaration of the termination.

[0248] When the client recognizes the reception of this response code (step S605), the TCP connection is cut off to terminate the current process.

(3-3) The Reception of the Electronic Mail

[0249] When an electronic mail is received by the POP 3 (Post Office Protocol version 3), for example, the POP client (hereinafter, simply referred to as a client) issues, at first, his request to the POP server (hereinafter, simply referred to as a server) for connection to receive the electronic mail as shown in Fig. 14 (step S611).

[0250] Then, the server returns to the client the response code indicating "connection OK" together with the name of the server.

[0251] Recognizing the reception of this response code and the name of the server (step S612), the client transmits to the server the name of the user and pass word for the server's identification by means of the USER command and the PASS command (step S613).

[0252] Then, when the server is able to confirm the user's name and pass word from the client, he returns to the client the response code indicating "normal".

[0253] Recognizing the reception of this response code (step S614), the client requests the server the information of the mail box (step S615) by means of the STAT command (the command whereby to request the information of

Ex.1002 / Page 259 of 1385
APPLE INC.

reception status of the mail box, such as numbers of mail), and the LIST command (the command whereby to request the list information of mails currently kept in the mail box) as required (step S615).

[0254] Then, the server transmits to the client the mail box information to comply with his request.

[0255] On the basis of the information received from the server, the client requests the server the transmission of the required mails (step S616).

[0256] Then, the server transmits to the client the required mails (step S617).

[0257] With the reception of mails from the server, he examines whether or not he has requested the server all the mails he needs (step S618). If it is found that there are still some more mails to be requested, then he returns to the process in the step S615, and repeats the processes thereafter.

[0258] If he has found that all the requested mails are received from the server as needed, he requests the server the execution of updating the mail box, and then, declares terminating his reception of the electronic mail by the POP 3 (step S619).

[0259] Then, the server returns to the client the response code indicating "termination" in accordance with the client's declaration of the termination.

[0260] When the client recognizes the reception of this response code (step S620), the connection of the POP 3 is cut off, and the current process is terminated.

[0261] Fig. 15 is the conceptual block diagram which shows the control flow for the digital camera 100 structured to perform various operations with the various function provided as described above, for example.

[0262] In other words, the digital camera 100 comprises a communication unit 301; the reception amount arithmetic unit 302 and the data storage 303 to which the output of the communication unit 301 is supplied, respectively; the memory 304 to which is supplied the output from the data storage 303; an image input unit 305; the image compression unit 306 to which is supplied the output from the image input unit 305; and the image storage unit 307 to which is supplied the output from the image compression unit 306. It is also arranged that the output of the image storage unit 307 is supplied to the memory 304.

[0263] The digital camera 100 further comprises the memory remainder arithmetic unit 309 to which is supplied the output from the memory 304; an input unit 310; the photographing mode setting unit 311 to which is supplied the output from the input unit 310; and the photographed image amount control unit 308 to which is supplied each of the outputs from the memory remainders arithmetic unit 309 and the photographing mode setting unit 311. It is also arranged that the output of the photographed image amount control unit 308 is supplied to the image compression unit 306.

[0264] Now, the communication unit 301 is the unit that corresponds to the PHS unit 203.

[0265] The reception amount arithmetic unit 302 is implemented by the application of software to be executed by the CPU 29 of the main CPU unit 201. The reception amount arithmetic unit 302 works out the data amount (the estimated amount of reception data) of the data expected to be received by the communication unit 301 using the communication protocol.

[0266] The data storage 303 stores the data received by the communication unit 301 on the memory 304 by use of the filing system.

[0267] The memory 304 corresponds to the flash ROM 32 (non-volatile memory) of the main CPU 201.

[0268] The image input unit 305 corresponds to the entire body of the camera unit 204 which is structured as shown in Fig. 6.

[0269] The image compression unit 306 is incorporated in the CPU 29, which is able to adjust the image size after compression by changing the designations as to the quantization table.

[0270] The image storage unit 307 stores the image data compressed by the image compression unit 306 on the memory 304 by the operation of the CPU 29.

[0271] The photographed image amount control unit 308 is implemented by the application of software used by the CPU 29.

[0272] More specifically, the compression control is carried out by changing the parameters of the quantization table or the like in the image compression unit 306. In other words, if it is determined that the remainders of the memory 304 are small by the indication of the memory remainders arithmetic unit 309, which will be described later, the image compression unit 306 is informed accordingly so that the image compression unit 306 may be able to change the compression ratios.

[0273] The memory remainders arithmetic unit 309 is implemented by the application of software used by the CPU 29, and when the remainders of the memory 304 are calculated, this unit uses the file system table arranged on the memory 304.

[0274] The input unit 310 corresponds to the mode dial 101. In other words, this unit is used when the photographer designates the photographing mode or the like.

[0275] The photographing mode setting unit 311 sets the photographing mode by notifying the current status of the mode dial 101 (input unit 310) to the CPU 29 by use of the sub-CPU 1 of the sub-CPU unit 202.

[0276] Here, the Table 1 shows one example of the photographing mode in which the modification is given to the

Ex.1002 / Page 260 of 1385
APPLE INC.

aforesaid image compression unit 306 by means 308 for controlling the photographed image amount, and the typical image sizes, as well as the numbers of the quantization table used at that time.

Table 1:

PHOTOGRAPHING MODE	SUPER FINE	FINE	NORMAL	ECONMY
Typical Size	200KB	100KB	50KB	25KB
QUANTIZING TABLE	1	2	3	4

[0277] Here, it is assumed that the photographing mode is classified into four stages: superfine mode, fine mode, normal mode, and economy mode, and that the image size after compression is classified into four stages: 400 KB, 200 KB, 100 KB, and 50 KB.

[0278] Now, hereunder, the description will be made of the processes executed by the application of software for controlling the photographed image amount.

[0279] On the ROM 32 of the main CPU unit 201, a program is stored in advance in accordance with the flowchart shown in Fig. 16, for example. When this program is read by the CPU 29 for execution, the amount of the photographed image is controlled for the digital camera 100 as given below.

[0280] At first, the communication unit 301 (PHS unit 203) determines whether or not the current status is the reception called (step S631), and also, whether or not the image input unit 305 (cameral unit 204) is in the photographing status (step S632).

[0281] As a result of this determination, if the status is the reception called in the photographing mode, the following steps will be executed. If not, the current process will be terminated.

[0282] Here, the determination of whether or not the status is in the photographing mode is made by the detection of the current status of the shutter button 102: whether it has been half depressed or totally depressed or by the detection of the CAMERA mode by means of the mode dial 101.

[0283] Then, if the reception call is ready in the photographing status, the photographed image amount control unit 308 obtains the value A (step S633) which is the value obtainable by subtracting the estimated amount of reception data calculated by the reception amount arithmetic unit 302 from the remainders of the memory 304 calculated by the memory remainders arithmetic unit 309.

[0284] Here, the estimated amount of reception data is worked out on the basis of the estimated amount of data on the received Email, for example. In other words, by use of the POP 3 described above as the communication protocol, the calculation is made by means of the POP 3 LIST command and STAT command in the "various information requests to the server" in the step S615 of the program shown in Fig. 14.

[0285] Now, the photographed image amount control unit 308 obtains from the aforesaid Table 1 the typical image size after compression corresponding to the current photographing mode set by the photographing mode setting unit 311. The image size thus obtained is subtracted from the value A that has been obtained in the step S633. After that, it is determined whether or not the resultant value exceeds a specific value (step S634).

[0286] Here, the reason why the value of the specific amount is used as offset is that the compression of the JPEG type or the like makes it difficult to estimate the image size after compression in advance, but to estimate only the typical image size after compression. Therefore, with the value of a specific amount which is set large enough, it becomes possible to secure a specific number of photographed images even after the termination of communication.

[0287] If the value obtained by subtraction should exceed the value of the specific amount as the result of the determination in the step S634, it means to indicate that there is still a room for the remainders of the memory 304. Therefore, the reception process, the photographing process, the compression process, and the recording process will be executed continuously (step S638). Then, the current process is terminated.

[0288] If the value obtained by subtraction does not exceed the value of the specific amount as the result of the determination in the step S634, it is determined by the photograph image amount control unit 308 whether or not there is any photographing mode applicable at a higher compression ratio by use of the aforesaid Table 1 in order to heighten the compression ratio of the image compression unit 306 (step S635).

[0289] If there is no photographing mode found that may serve the purpose as the result of the determination in the step S635, the reception operation is suspended (step S637), and the current process is terminated.

[0290] Here, as to the photographing operation, it is assumed that the photographing operation is started after the remainders of the memory 304 have been detected and confirmed. Therefore, it is possible to continue the photographing operation even if there is no suitable photographing mode found applicable as the result of the determination in the step S635.

[0291] If the corresponding photographing mode has been found as the result of the determination in the step S635, the photographed image amount control unit 308 heightens the compression ratio of the image compression unit 306

Ex.1002 / Page 261 of 1385
APPLE INC.

(step S636) by directing the image compression unit 306 to the quantization table applicable to the photographing mode that may be obtained from the aforesaid Table 1.

[0292] Subsequently, the process returns to the step S634, and repeats the processing steps thereafter.

(Second Embodiment)

[0293] The structure of the digital camera of the present embodiment is the same as that of the digital camera 100 in the accordance with the first embodiment described above. However, the control of the entire body is different.

[0294] In other words, as shown in Fig. 15, the communicating operation of the compunction unit 301 and the photographing operation of the image input unit 305 are overlapped. Therefore, if the remainders of the memory 304 become insufficient, the amount of the reception data from the communicating party is controlled (restricted) by use of the communication protocol.

[0295] Consequently, the structure (the conceptual structure shown in the block diagram) of the digital camera 100 shown in Fig. 15 is modified to be the one shown in Fig. 17, for example.

[0296] As shown in Fig. 17, the reception amount control unit 321 is arranged in place of the photographed image amount control unit 308 shown in Fig. 15.

[0297] The reception amount control unit 321 is implemented by the application of software of the CPU 29 to receive each of the outputs supplied from the reception amount arithmetic unit 302 and the memory remainders arithmetic unit 309, and to output its processed data to the communication unit 301.

[0298] Also, the reception amount control unit 321 receives the information of the remainders of the memory 304 from the memory remainders arithmetic unit 309, and if it is determined that the amount of the reception data is large, this unit notifies the communication unit 301 accordingly so as to restrict the amount of reception data to be received by the communication unit 301. More specifically, using the communication protocol this unit notifies the communicating party of its denial of the reception of data, partly or otherwise, through the communication unit 301.

[0299] Now, hereunder, the description will be made of the processes executed by the application of software to control (restrict) the amount of reception data.

[0300] Here, in this respect, the specific description will be made of the aspects which differ from those of the first embodiment.

[0301] On the ROM 32 of the main CPU unit 201, a program is stored in advance in accordance with the flowchart shown in Fig. 18, for example. When this program is read by the CPU 29 for execution, the control (restriction) of the amount of reception data is performed for the digital camera 100 as given below.

[0302] At first, in the same manner as in step S631 to step S634 shown in Fig. 16, it is determined whether or not the current status is the reception called or whether or not the current status is the photographing (step S641 and step S642). If it is found that both the reception called and the photographing are ready, the following steps will be executed for processing. If not, the current process is terminated.

[0303] In the reception called status, and also, in the photographing status, the reception amount control unit 321 obtains the value A which is arrived at by subtracting the estimated amount of reception data calculated by the reception amount arithmetic unit 302 from the amount of the memory remainders calculated by the memory remainders arithmetic unit 309 (step S643).

[0304] Then, the reception amount control unit 321 obtains from the aforesaid Table 1 the typical image size after compression corresponding to the current photographing mode set by the photographing mode setting unit 311. The image size thus obtained is subtracted from the value A obtained in the step S643 to determine whether or not the resultant value exceeds the value of a specific amount (step S644).

[0305] If it is found that the subtracted value exceeds the value of the specific amount as the result of determination in the step S644, this indicates that there is still room for the remainders of the memory 304. Therefore, the reception process, the photographing process, the compression process, and the recording process are continuously executed (step S648). Then, the current process will be terminated.

[0306] Here, if it is not found that the subtracted value exceeds the value of the specific amount as the result of determination in the step S644, the reception amount control unit 321 inquires to the communicating party whether or not the transmission is still possible with a higher compression ratio through the communication unit 301 (step S645).

[0307] If it is found in the step S645 that the transmission with a higher compression ratio is impossible on the communicating party side, the reception operation is suspended (step S647), and then, the current process will be terminated.

[0308] As described above, it is determined, at first, whether or not the current status is the reception called or photographing (step S641 and step S642). If affirmative, the processes in the step S643 and on are executed. If negative, the processes will be executed in the step S702 and on as described later.

[0309] In the reception called status, and also, in the photographing status, the reception amount control unit 321 obtains the value A which is arrived at by subtracting the estimated amount of reception data calculated by the reception

Ex.1002 / Page 262 of 1385
APPLE INC.

amount arithmetic unit 302 from the amount of the memory remainders calculated by the memory remainders arithmetic unit 309 (step S643).

[0310] Here, the estimated amount of the reception data is calculated by means of the required commands whereby to request various information from the server. For example, the POP 3 LIST command and STAT command are used as described in the paragraphs of "(3-3) Electronic Mail Reception".

[0311] Then, the reception amount control unit 321 obtains from the aforesaid Table 1 the typical image size after compression corresponding to the current photographing mode set by the photographing mode setting unit 311. The image size thus obtained is subtracted from the value A obtained in the step S643 to determine whether or not the resultant value exceeds the value of a specific amount (step S644).

[0312] Here, the reason why the "value of a specific amount" is used as offset is that the compression of the JPEG type or the like makes it difficult to estimate the image size after compression in advance, but to estimate only the typical image size after compression.

[0313] In this respect, if only the value of a specific amount should be set large enough, it becomes possible to secure a specific number of photographed images even after the termination of communication.

[0314] If the value obtained by subtraction should exceed the value of the specific amount as the result of the determination in the step S644, it means to indicate that there is still a room for the remainders of the memory 304. Therefore, the reception process, the photographing process, the compression process, and the recording process will be executed continuously (step S648). Then, the process proceeds to step S702 shown in Fig. 19, which will be described later.

[0315] On the other hand, if it is not found as the result of the determination in the step S644 that the subtracted value exceeds the value of the specific amount, this means to indicate that it is impossible to take a margin for the size of a specific image. Thus, the reception amount control unit 321 inquires to the communicating party whether or not the transmission is still possible with a higher compression ratio (step S645).

[0316] If it is found in the step S645 that the transmission with a higher compression ratio is impossible on the communicating party side, the reception operation is suspended (step S647).

[0317] Then, the process will proceed to step S702, which will be described later.

[0318] Here, the photographing operation will be continued for the reason described above.

[0319] If it is determined in the step S645 that the transmission with a higher compression is possible on the communicating party side, the control is made to change the compression and expansion type by the communication unit 301 (the reception side) and by the communicating party side (transmission side) as well. At this juncture, the retransmission flag (inner flag) is set in the communication unit 301 (step S646).

[0320] After that, the process will return to the step S644, and repeat the processing steps thereafter.

(Third Embodiment)

[0321] In the step S702, the communication unit 301 examines if the retransmission flat is set or not.

[0322] As a result of this examination, if the retransmission flat is not set, the communication unit 301 issues to the communicating party the request of the original data retransmission. In this case, the request of the retransmission of the original data is made after promoting the user to increase the remainders of the memory or after the remainders of the memory have been increased, for example. In this way, it is possible to prevent the shortage of memory remainders when receiving the original data for the normal execution of the original data reception (step S703).
After that, the retransmission flag is reset to terminate the current process.

[0323] On the other hand, if the retransmission flag is not set in the step S702, the current process will be terminated as it is.

(Fourth Embodiment)

[0324] For the second embodiment described above, it is arranged to control (restrict) the amount of the reception data by changing the compression and expansion type (see steps S645 and S646 in Fig. 18). In accordance with the present embodiment, only a part of the data (original data) that should be transmitted totally is received, and then, the remaining part will be received after a photographing is completed. In this manner, the amount of the reception data will be controlled (restricted).

[0325] Therefore, as the program executed by the CPU 29, a program prepared in accordance with the flowchart shown in Fig. 20 is used, for example, in place of the program shown in Fig. 18. The control is then made in accordance with the present embodiment.

[0326] Here, the same reference marks as those appearing in the flowchart shown in Fig. 18 are applied to the same processing steps of the flowchart shown in Fig. 20, and the detailed description will be omitted. In this respect, the specific description will be made only of the structure which differs from that of the second embodiment.

Ex.1002 / Page 263 of 1385
APPLE INC.

[0327] At first, it is determined whether or not the current status is the reception called or whether or not the current status is the photographing (step S641 and step S642). As a result thereof, if it is found that both the reception called and photographing status are ready, the next processing step S643 and on will be executed. If not, the processing steps will be executed beginning with the step S712 which will be described later.

[0328] With the status being the reception called and the photographing, the reception amount control unit 321 obtains the value A (step S643) by subtracting the estimated amount of reception data calculated by the reception data arithmetic unit 302 form the amount of memory remainders calculated by the memory remainders arithmetic unit 309 (step S643).

[0329] Then, the reception amount control unit 321 subtracts the typical image size after compression corresponding to the current photographing mode set by the photographing mode setting unit 311 from the value A obtained in the step S643, and determines whether or not the result thereof exceeds the value of a specific amount (step S644).

[0330] As a result of the determination in the step S644, if the subtracted value exceeds the value of the specific amount, this means to indicate that there is still a room for the remainders of the memory 304. Therefore, the reception process, the photographing process, the compression process, and recording process will be continued (step S648).

[0331] Then, the process will proceed to the step S712 which will be described later.

[0332] On the other hand, if the subtracted value does not exceed the value of the specific amount as the result of the determination in the step S644, this means to indicate that no margin is obtainable for the specific size of an image. Therefore, the reception amount control unit 321 controls the communication unit 301 so as to receive only a part of all the data which are expected to be sent from the communicating party. For example, if it is the case of an electronic mail, only the "headings" are requested for reception. Also, in the communication unit 301, the retransmission flag (inner flag) is set (step S711).

[0333] If the structure is made in this manner so that only a part of the original data is received from the communicating party side, some more room is created in the memory remainders. Thus, the aforesaid step S648 is made executable. As a result, the reception process, the photographing process, the compression process, and the recording process will be executed continuously (step S648).

[0334] After that, the process will proceed to step S712.

[0335] In the step S712, the communication unit 301 examines if the retransmission flag has been set.

[0336] It is found as the result of this examination that the retransmission flag has been set, the communication unit 301 issues to the communicating party the request of retransmission of the remaining data. In this case, such request of retransmission is issued after having prompted the user to increase the memory remainders or after the remainders of the memory have been increased. Then, it becomes possible to prevent the incapability of securing the remainders of the memory large enough to receive the original data or the occurrence of some other related problems. In this way, the original data can be received normally at all times (step S713). After that, the retransmission flag is reset, and the current process will be terminated.

[0337] On the other hand, if it is not found that the retransmission flag is set, the current process will be terminated as it is.

(Fifth Embodiment)

[0338] In the third embodiment described above, the arrangement is made so that if it is determined that the transmission is possible at a higher compression ratio on the communicating party side (step S645), the data is transmitted with the modified compression ratio against the amount in which the data should be sent originally (step S701), and, therefore, when the connection is made again after the completion of the current photographing, the request of retransmission of the data is issued (step S703) with respect to the data which should have been sent originally before (see Fig. 19).

[0339] In accordance with the present embodiment, when the retransmission request is issued in such a case described above, the image data that has been photographed is transmitted to the communicating party, and then, the retransmission request is issued as shown in Fig. 21 (step S731)

[0340] In this way, with the transmission of the photographed data (photographed image data obtained by photographing) to the communicating party, the image data that has been in the corresponding unit can be deleted. This in return makes it possible to increase the memory remainders to that extent. Then, it becomes possible to prevent the incapability of securing the memory remainders large enough to receive the original data from the communicating party or occurrence some other related problems.

(Sixth Embodiment)

[0341] The digital camera of the present embodiment is structured in the same manner as the digital camera 100 described in the second embodiment. However, the control of the entire body thereof is different.

Ex.1002 / Page 264 of 1385
APPLE INC.

[0342] In other words, when the reception is made as to the audio, image, and other streaming data which make the estimate of reception data amount difficult, it is arranged to issue the denial of communication.

[0343] Now, hereunder, the description will be made of the application of software to be used for the reception of streaming data.

[0344] In this respect, only what differs from the second embodiment will be described specifically.

[0345] On the ROM 32 of the main CPU unit 201, a program is stored in advance in accordance with the flowchart shown in Fig. 22, for example. When this program is read by the CPU 29 for execution, the control is made for the digital camera 100 as to the reception of streaming data as given below.

[0346] At first, in the same manner as in the step S641 to step S643 shown in Fig. 18, it is determined whether or not the status is the reception called or whether or not the status is the photographing (step S651 and step S652). As the result of this determination, if the status is found to be the reception called and the photographing as well, the following processing steps will be executed. If not the current process will be terminated.

[0347] Then, in the case of the reception called and photographing statuses, the reception amount control unit 321 obtains the value A by subtracting the estimated amount of reception data calculated by the reception amount arithmetic unit 302 from the remainders of memory 304 calculated by the memory remainders arithmetic unit 309 (step S653).

[0348] Now, the reception amount control unit 321 determines whether or not the estimated amount of reception data calculated by the reception amount arithmetic unit 302 is of the streaming data (step S654).

[0349] As the result of the determination in the step S654, if it is found that the data is the streaming one, that is, if the data expected to be received is such as recorded telephone conversations, the reception operation is suspended (step S657). Then, the current process will be terminated.

[0350] This is because if the data is the streaming one, it is difficult to estimate the data amount or even if the estimate is possible, the function whereby to restrict the amount of the reception data as described above may result in the structure which becomes simply awkward for the user to use eventually.

[0351] As the result of the determination in the step S654, if it is not found that the data is not the streaming one, the reception amount control unit 321 obtains the typical image size after compression from the aforesaid Table 1 corresponding to the current photographing mode set by the photographing mode setting unit 311 as shown in Fig. 18. Then, the image size thus obtained is subtracted from the value A obtained in the step S643 to determine whether or not the resultant value exceeds the value of a specific amount (step S655).

[0352] If it is found that the subtracted value exceed the value of the specific amount as the result of the determination in the step S655, this means to indicate that there is still a room for the remainders of memory 304. Thus, the reception process, the photographing process, the compression process, and the recording process will be performed continuously (step S658). After that, the current process will be terminated.

[0353] If it is not found as the result of the determination in the step S655 that the subtracted value exceeds the value of the specific amount, the reception operation is suspended (step S657). Then, the current process will be terminated.

[0354] In this respect, it is of course possible to achieve the objectives of the present invention by supplying to a system or to an apparatus, a storage medium on which the codes of application programs are recorded to implement the host and the terminals in accordance with each of the embodiments described above so that the computer (or CPU or MPU) of such system or apparatus is arranged to be able to read such stored programming codes on the storage medium for execution.

[0355] In this case, the programming codes themselves thus read from the storage medium implement each of the functions of the respective embodiments. Therefore, it is to be understood that the storage medium on which the aforesaid programming codes constitutes the present invention.

[0356] As the storage medium that may be able to supply the programming codes, there are ROM, floppy disc, hard disc, optical disc, magnet-optic disc, CD-ROM, CD-R, magnetic tape, non-volatile memory card, and some other that can be used.

[0357] Also, it is to be understood that the present invention includes the case as a matter of course where not only the functions of the respective embodiments described above can be implemented by the execution of the programming codes read out by the computer, but also, the functions of the respective embodiments can be implemented by the processes executed by the OS or others operating in the computer which perform the actual processes partly or totally in accordance with the instructions from such programming codes.

[0358] Moreover, it is to be understood that the present invention includes the case as a matter of course where the programming codes are read from the storage medium and written on the memory of an extended function board inserted into the computer or on the memory of the extended functional unit connected with the computer, and then, the CPU or the like provided for such extended function board or the extended functional unit performs the actual processes partly or totally in accordance with the instructions from the aforesaid programming codes, hence implementing the functions of the respective embodiments described above by means of such processes.

[0359] Also, as to the intervention operation of intervention means of the present invention (or the control operation of control means), the present invention is not necessarily limited to those described in the respective embodiments.

Ex.1002 / Page 265 of 1385
APPLE INC.

For example, it may be possible to save the image data simply on the buffer memory which is arranged to delay the image input of the digital cameral or the like temporarily.

[0360] Also, as to the changes of the reception data in accordance with the present invention, it may be possible to structure the arrangement so that the reception data is again compressed by the application of the data compression algorithm (ZIP method or the like used for a personal computer) for example, not necessarily limited to those described in the respective embodiments.

[0361] In accordance with the present invention described above, it becomes possible to overcome the disadantages or the like that the collision of memory resources may take place when a digital camera and a communication device are integrally formed for use with the arrangement to control the functions such as the automatic changes of compression ratio and the automatic changes of the sizes of reception data.

[0362] Consequently, it is possible to satisfy the communication having a high immediacy, and the photographing having a high immediacy as well at the same time. Furthermore, it becomes possible to provide a smaller apparatus or a smaller system having a higher operativity.

[0363] Also, on the photographing site, there is no possibility that the photographer misses his shutter change. At the same time, he is able to perform his photographing quickly and to make a highly reliable communicate with his party or parties.

[0364] Moreover, since such controls as have been described above are implemented by controlling the apparatus, the CPUs, memories, and others, the structure can be formed simply so as to perform the controls with the transmission device having the usual structure, the digital camera provided with an interface for transmission use, or the like.

[0365] Also, when the data transmission is performed on the transmission side with the compression ratio which has been increased, it is possible to obtain the data that should have been sent originally if it is structured that the retransmission request may be issued after the completion of photographing.

[0366] In this case, the photographed image data (the photographed image obtained and stored in an apparatus or a system) is at first transmitted to the transmission side, and then, such controls as have been described above may be performed.

[0367] In this way, the remainders of memory is increased so that the data are received reliably from the transmission side.

[0368] With these features and advantages, the present invention should be significantly useful at present and in future, because the image input is possible with a high immediacy by the combination of communication, photographing, and some others, and at the same time, the apparatus is made smaller at low power dissipation and at lower costs of manufacture.

[0369] Now, various inventions have been shown in accordance with the embodiments described above. Here, besides the embodiments referred to in the paragraphs of the Summary of the Invention, there are still more embodiments as given below.

Item 6:

[0370] For example, in accordance with the other embodiments, a method of the present invention for processing images comprises the steps of performing the reception of data through the net work; inputting image data obtainable in accordance with the designated input mode; managing step of managing the storage of the data received in the receiving step and the image data inputted in the input step to the memory; and the step of intervening between the operations of the reception step and the input step in accordance with the storage management.

[0371] In this way, the data reception operation and the image input operation are controlled in accordance with the current status of memory storage. Therefore, it becomes possible to deal with any sudden reception or the like during the storing operation of the image data on the memory, hence making the compatibility possible with respect to the immediacy of the image input, and the communication as well.

Item 7:

[0372] Also, the reception step further comprises the step of receiving data through wireless net work.

[0373] In this manner, this method is arranged to be able to deal with communications on the wireless net work. Item 8:

[0374] Also, the intervening step controls the input mode in the input step in accordance with the storage management.

[0375] In this manner, the method is arranged to be able to control the storing operation of the image data on the memory by changing the current input modes depending on the condition of the memory storage. Item 9:

[0376] Now, the aforesaid input step further comprises an image inreversible compression step, and the intervening means controls the compression ratio in the compression step.

[0377] In this manner, the method is arranged to control the amount of image data to be stored on the memory by

Ex.1002 / Page 266 of 1385
APPLE INC.

changing the compression ratios depending on the current status of the memory storage.

Item 10:

[0378] Furthermore, the managing means manages the remaining amount of the memory.

[0379] Hence, the method is arranged to control the data reception operation and the image input operation in accordance with the remaining capacity of the memory storage.

Item 11:

[0380] Here, there are still other embodiments as given below.

[0381] An image input apparatus, which is provided with the communicating function, and storing on storage means an input image obtainable in accordance with the reception data provided by the communicating function and inputted in the photographing mode designated in advance, comprises image compression means for storing the storage means the input image at the compression ratio corresponding to the photographing means; reception amount generating means for obtaining the capacity required for the data reception by the communicating function; remainders generating means for obtaining the memory remainders for the storage means; and control means for controlling the compression ratios of the image compression means in accordance with the capacity obtained by the reception amount generating means, and the memory remainders obtained by the remainder generating means.

[0382] In this way, this apparatus is arranged to be able to heighten the compression ratio of the image compression means by changing the current photographing modes if, for example, the added value of the required capacity (estimated reception size) for the data reception and the data size of the input images predetermined by the current photographing mode (photographing quality mode) should be larger than the memory remainders. Therefore, it is possible to deal with any sudden reception during photographing, thus implementing the compatibility of immediacy between the photographing and communication.

Item 12:

[0383] Also, an image input apparatus comprises input means for inputting the photographing mode; image input means for inputting an image obtained by the photographing mode inputted by the input means; image compression means for compressing the input image inputted by the image input means; communicating means for receiving arbitrary data; storage means for storing the input image compressed by the image compression means and the data received by the communicating means; remainder generating means for managing memory remainders of the storage means; and control means for controlling the compression ratios of the image compression means in accordance with the capacity obtained by the reception amount generating means, and the memory remainders obtained by the remainder generating means.

[0384] In this way, this apparatus is arranged to be able to compare the added value of the required capacity (estimated reception size) for the data reception and the data size of the input images predetermined by the current photographing mode (photographing quality mode) with the memory remainders currently available, and then, if it is found by the result of this comparison that such added value is larger than the memory remainders, the photographing mode is automatically changed so as to heighten the compression ratio to deal with any sudden reception during photographing. As a result, it becomes possible to implement conveniently the compatibility of immediacy between the photographing and communication.

Item 13:

[0385] An image input apparatus, which is provided with the communicating function, and storing on storage means an input image obtainable in accordance with the reception data provided by the communicating function and inputted in the photographing mode designated in advance, comprises reception amount generating means for obtaining the required capacity for receiving data by the communicating function; remainders generating means for obtaining the memory remainders for the storage means; and control means for controlling the receiving operation of the communicating function in accordance with the capacity obtained by the reception amount generating means, and the memory remainders obtained by the remainder generating means.

[0386] In this way, it becomes possible to receive only a part of the estimated reception data in advance or heighten the compression ratio of the reception data in order to make the size of the reception data smaller if, for example, the added value of the required capacity (estimated reception size) for the data reception and the data size of the input images predetermined by the current photographing mode (photographing quality mode) should be larger than the memory remainders. Therefore, it is possible to deal with any sudden reception during photographing, thus implement-

Ex.1002 / Page 267 of 1385
APPLE INC.

ing the compatibility of immediacy between the photographing and communication.

Item 14:

[0387] An image input apparatus comprises input means for inputting the photographing mode; image input means for inputting an image obtained by the photographing mode inputted by the input means; image compression means for compressing the input image inputted by the image input means; communicating means for receiving arbitrary data; storage means for storing the input image compressed by the image compression means and the data received by the communicating means; remainder generating means for managing memory remainders of the storage means; reception amount generating means for obtaining the required capacity for receiving data by the communicating function; and control means for controlling the amount of reception data of the communicating means in accordance with the memory remainders obtained by the remainder generating means, and the capacity obtained by the reception amount generating means.

[0388] In this way, this apparatus is arranged to be able to compare the added value of the required capacity (estimated reception size) for the data reception and the data size of the input images predetermined by the current photographing mode (photographing quality mode) with the memory remainders currently available, and then, if it is found by the result of this comparison that such added value is larger than the memory remainders, the apparatus deals with any sudden reception during the photographing. More specifically, the apparatus performs the control so as to receive only a part of the estimated reception data or to heighten the compression ratio thereof, among some other controls. As a result, it becomes possible to implement conveniently the compatibility of immediacy between the photographing and communication.

Item 15:

[0389] The aforesaid control means described in the item 13 or item 14 restricts the reception data if the added value of the capacity obtained by the reception amount generating means and the estimated size of the input image defined in advance by the photographing mode is larger than the memory remainders of the storage means.

[0390] Here, in this case, the amount of the reception data is restricted by the denial of the communication during the photographing or by some other means so as to enable the photographer to materialize his intention satisfactorily.

Item 16:

[0391] The aforesaid control means described in the item 13 or item 14 restricts the amount of the reception data if the added value of the capacity obtained by the reception amount generating means and the estimated size of the input image defined in advance by the photographing mode is larger than the memory remainders of the storage means, and after that, the retransmission request of data is issued to the transmission side.

Item 17:

[0392] The aforesaid control means described in the item 13 or item 14 enables the transmission side to transmit the data having higher compression ratio if the added value of the capacity obtained by the reception amount generating means and the estimated size of the input image defined in advance by the photographing mode is larger than the memory remainders of the storage means.

Item 18:

[0393] The aforesaid control means described in the items 15 to 17 transmits to the transmission side the input. image stored on the storage means.

Item 19:

[0394] The aforesaid control means described in the item 13 or item 14 controls the reception denial when the reception data is the streaming data corresponding to the capacity obtained by the reception amount generating means.

[0395] Here, in this case, even if the reception of the streaming data (for example, the real time reception of conversations or some other streaming data) suddenly takes place during photographing, such reception is denied completely. Therefore, the priority is given to the fulfillment of the user's intention.

Ex.1002 / Page 268 of 1385
APPLE INC.

Item 20:

[0396] The aforesaid control means described in the item 13 or item 14 controls the amount of the reception data when the added value of the data size of the predetermined numbers of input images, the capacity obtained by the reception amount generating means, and the estimated size of the input images predetermined by the photographing mode is larger than the memory remainders.

[0397] In this way, even if it is required that the communication and photographing should coexist for the intended operation, the area needed for the estimated numbers of images to be recorded is secured at all the time. Therefore, the photographer is able to concentrate his attention on photographing.

Item 21:

[0398] There is provided an image processing apparatus described in any one of the item 6 to item 10 or an image input device described in any one of the items 11 to 20.

[0399] Here, it becomes possible to provide a photographing apparatus capable of implementing the compatibility of immediacy between the photographing and communication.

Item 22:

[0400] There is provided an image processing apparatus described in any one of the item 6 to item 10 or an image input device described in any one of the items 11 to 20.

[0401] Here, it becomes possible to provide a photographing system capable of implementing the compatibility of immediacy between the photographing and communication.

Item 23:

[0402] There is provided an image processing apparatus described in any one of the item 6 to item 10 or an image input device described in any one of the items 11 to 20.

[0403] Here, it becomes possible to provide a communicating device capable of implementing the compatibility of immediacy between the photographing and communication.

Item 24:

[0404] There is provided an image processing apparatus described in any one of the item 6 to item 10 or an image input device described in any one of the items 11 to 20.

[0405] Here, it becomes possible to provide a communicating system capable of implementing the compatibility of immediacy between the photographing and communication.

Item 25:

[0406] A storage medium, which is provided with the processing steps readable by a computer on the memory, stores the input images obtainable by being inputted by the communicating function, the reception data through the communicating function, and the photographing mode designated in advance. The aforesaid processing steps comprises the steps of compressing images to be stored on the memory by compressing the input images with the compression ratio corresponding to the photographing mode; generating the reception amount for obtaining the required capacity for the data reception by the communicating function; generating remainders for obtaining the memory remainders of the memory; and controlling the compression ratio in the image compressing step in accordance with the photographing mode, the capacity obtained in the reception amount generating step, and the memory remainders obtained in the remainders generating step.

[0407] In this way, it is possible to heighten the compression ratio of the input images by changing the current photographing modes if, for example, the added value of the required capacity (estimated reception size) for the data reception and the data size of the input images predetermined by the current photographing mode (photographing quality mode) should be larger than the memory remainders. Therefore, it becomes possible to deal with any sudden reception during photographing, thus providing an apparatus or a system capable of implementing the compatibility of immediacy between the photographing and communication.

Ex.1002 / Page 269 of 1385
APPLE INC.

Item 26:

[0408] A storage medium, which is provided with the processing steps readable by a computer, stores on memory the input images obtainable by being inputted by the communicating function, the reception data through the communicating function, and the photographing mode designated in advance. The aforesaid processing steps comprises the steps of generating the reception amount for obtaining the required capacity for the data reception by the communicating function; generating the remainders for obtaining the memory remainders of the memory; controlling the compression ratio in the image compressing step in accordance with the photographing mode, the capacity obtained in the reception amount generating step, and the memory remainders obtained in the remainders generating step.

[0409] In this manner, it is possible to receive only a part of the estimated reception data and heighten the compression ratio of the input images by changing the current photographing modes if, for example, the added value of the required capacity (estimated reception size) for the data reception and the data size of the input images predetermined by the current photographing mode (photographing quality mode) should be larger than the memory remainders. Therefore, it becomes possible to make the size of the reception data smaller to deal with any sudden reception during photographing, thus providing an apparatus or a system capable of implementing the compatibility of immediacy between the photographing and communication.

Item 27:

[0410] A storage medium described in the item 26, the aforesaid the controlling step comprises the step of restricting the amount of reception data if the added value of the capacity obtained in the reception amount generating step and the estimated size of input images predetermined by the photographing mode is larger than the memory remainders.

[0411] Here, in this case, the amount of the reception data is restricted by the denial of the communication during the photographing or by some other means so as to enable the photographer to materialize his intention satisfactorily.

Item 28:

[0412] The aforesaid controlling step described in the item 26 controls the reception denial when the reception data is the streaming data corresponding to the capacity obtained in the reception amount generating step.

[0413] Here, in this case, even if the reception of the streaming data (for example, the real time reception of conversations or some other streaming data) suddenly takes place during photographing, such reception is denied completely. Therefore, the priority is given to the fulfillment of the user's intention.

Item 29:

[0414] The aforesaid the controlling step described in the item 26 comprises the step of restricting the amount of reception data when the added value of the data size of the predetermined numbers of input images, the capacity obtained by the reception amount generating step, and the estimated size of the input images predetermined by the photographing mode is larger than the memory remainders.

[0415] In this way, even if it is required that the communication and photographing should coexist for the intended operation, the area needed for the estimated numbers of images to be recorded is secured at all the time. Therefore, the photographer is able to concentrate his attention on photographing.

Item 30:

[0416] A storage medium stores the processing step of image processing method according to either one of the item 1 to item 5 so as to make in readable by a computer.

[0417] In this manner, it becomes possible to provide an apparatus or a system capable of implementing the compatibility of immediacy between the image input and the communication.

Claims

1. An image processing method comprising the steps of:

receiving data through a net work;
inputting image data obtained in accordance with a designated input mode;
managing storage of the data received in said receiving step and the image data inputted in said input step

Ex.1002 / Page 270 of 1385
APPLE INC.

to a memory; and
intervening between operations of said reception step and said input step on the basis of said storage management in said managing step.

2. A method according to Claim 1, wherein said receiving step further comprises a step of receiving data through wireless net work.

3. A method according to Claim 1, wherein said intervening step further comprises the control step of controlling the input mode in said inputting step on the basis of said storage management in said managing step.

4. A method according to Claim 1, wherein said inputting step further comprises an image inreversible compression step, and wherein said intervening step further comprises a control step for controlling a compression ratio in said compression step.

5. A method according to Claim 1, wherein said managing step further comprises a step of managing a remaining storage capacity of said memory.

6. A method comprising the steps of:

receiving data through a net work;
inputting image data obtained in accordance with the designated input mode;
managing storage of the data received in said receiving step and the image data inputted in said inputting step to a memory; and
intervening between operations of said receiving step and said inputting step on the basis of said storage management.

7. A method according to Claim 6, wherein said reception step further comprises a step of receiving data through wireless net work.

8. A method according to Claim 6, wherein said intervening step controls the inputting mode in said inputting step in accordance with said storage management.

9. A method according to Claim 6, wherein said input step further comprises an image inreversible compression step, and said intervening means controls a compression ratio in said compression step.

10. A method according to Claim 6, wherein said managing means manages a remaining amount of said memory.

11. An image input apparatus having a communicating function, and for storing into storage means data received by said communicating function and an image inputted in a photographing mode designated in advance, comprising:

image compression means for storing into said storage means the input image at a compression ratio corresponding to the photographing mode;
reception amount generating means for obtaining a capacity required for a data reception by said communicating function;
remaining amount generating means for obtaining the memory remaining amount for said storage means; and
control means for controlling the compression ratio of said image compression means on the basis of the capacity obtained by said reception amount generating means, and the memory remaining amount obtained by said remaining amount generating means.

12. An image input apparatus, comprising:

input means for inputting a photographing mode;
image input means for inputting an image obtained in the photographing mode inputted by said input means;
image compression means for compressing the image inputted by said image input means;
communicating means for receiving arbitrary data;
storage means for storing the input image compressed by said image compression means and the data received by said communicating means;
remaining amount generating means for managing memory remaining amount of said storage means; and

Ex.1002 / Page 271 of 1385
APPLE INC.

control means for controlling an amount of the input image for said image compression means on the basis of photographing mode inputted by said input means, and the memory remaining amount obtained by said remaining amount generating means.

13. An image input apparatus having the communicating function, and for storing into storage means data received by said communicating function and an image inputted in the photographing mode designated in advance, comprising:

reception amount generating means for obtaining a capacity required for receiving data by said communicating function;
remaining amount generating means for obtaining a memory remaining amount for said storage means; and
control means for controlling a receiving operation of said communicating function on the basis of the capacity obtained by said reception amount generating means, and the memory remaining amount obtained by said remaining amount generating means.

14. An image input apparatus, comprising:

input means for inputting a photographing mode;
image input means for inputting an image obtained in the photographing mode inputted by said input means;
image compression means for compressing the input image inputted by said image input means;
communicating means for receiving arbitrary data;
storage means for storing the input image compressed by said image compression means and the data received by said communicating means;
remaining amount generating means for managing memory remaining amount of said storage means;
reception amount generating means for obtaining a capacity required for receiving data by said communicating function; and
control means for controlling the amount of reception data of said communicating means on the basis of the memory remaining amount obtained by said remaining amount generating means, and the capacity obtained by said reception amount generating means.

15. An image input apparatus according to Claim 13, wherein said control means restricts the reception data when an added value of the capacity obtained by said reception amount generating means and an estimated size of the input image defined in advance in said photographing mode is larger than the memory remaining amount of said storage means.

16. An image input apparatus according to Claim 13, wherein said control means restricts the amount of the reception data when an added value of the capacity obtained by said reception amount generating means and the estimated size of the input image defined in advance in said photographing mode is larger than the memory remaining amount of said storage means, and after that, a retransmission request of data is issued to a transmission side.

17. An image input apparatus according to Claim 13, wherein said control means enables the transmission side to transmit the data having higher compression ratio when an added value of the capacity obtained by said reception amount generating means and the estimated size of the input image defined in advance by said photographing mode is larger than the memory remaining amount of said storage means.

18. An image input apparatus according to Claim 15, wherein said control means transmits to a transmission side the input image stored into said storage means.

19. An image input apparatus according to Claim 13, wherein said control means controls the reception denial when the reception data corresponding to the capacity obtained by said reception amount generating means is streaming data.

20. An image input apparatus according to Claim 13, wherein said control means controls the amount of the reception data when the added value of the data size of the predetermined numbers of input images, the capacity obtained by said reception amount generating means, and an estimated size of the input images predetermined in said photographing mode is larger than the said memory remaining amount.

21. An image pickup apparatus provided with the image processing apparatus according to Claim 6.

Ex.1002 / Page 272 of 1385
APPLE INC.

22. An image pickup system provided with the image processing apparatus according to Claim 6.

23. A communicating apparatus provided with the image processing apparatus according to Claim 6.

24. A communicating system provided with the image processing apparatus according to Claim 6.

25. A storage medium which stored processing steps readable by a computer, for storing on memory a communicating function, reception data by the communication function, and an image inputted in a photographing mode designated in advance, said processing steps comprising the following steps of:

compressing the input image with a compression ratio corresponding to the photographing mode and storing the compressed image;
generating reception amount for obtaining a capacity required for the data reception by said communicating function;
generating remaining amount for obtaining the memory remaining amount of said memory; and
controlling the compression ratio in said image compressing step on the basis of said photographing mode, the capacity obtained in said reception amount generating step, and the memory remaining amount obtained in said remaining amount generating step.

26. A storage medium which stored the processing steps readable by a computer for storing a communicating function, the reception data by said communicating function, and an image inputted in the photographing mode designated in advance, said processing steps comprising the following steps of:

generating the reception amount for obtaining a capacity required for the data reception by said communicating function;
generating the remaining amount for obtaining the memory remaining amount of said memory;
controlling a receiving operation by the comunication function on the basis of said photographing mode, the capacity obtained in said reception amount generating step, and the memory remaining amount obtained in said remaining amount generating step.

27. A storage medium according to Claim 26, wherein said controlling step comprises the step of restricting an amount of reception data when the added value of the capacity obtained in said reception amount generating step and the estimated size of input image predetermined in said photographing mode is larger than said memory remaining amount.

28. A storage medium according to Claim 26, wherein said controlling step controls the reception denial when the reception data corresponding to the capacity obtained in said reception amount generating step is streaming data.

29. A storage medium according to Claim 26, wherein said controlling step comprises the step of restricting the amount of reception data when the added value of the data size of the predetermined numbers of input images, the capacity obtained in said reception amount generating step, and the estimated size of the input images predetermined in said photographing mode is larger than the said memory remaining amount.

30. A storage medium which stored the processing step of image processing method according to either one of Claim 1 to Claim 5 in being readable by a computer.

31. A digital camera in combination with a wireless data communication device for receiving or transmitting data, and storage means for storing both images and received data.

32. A digital camera according to claim 31 and including switch means for switching between a plurality of modes, one mode being an image taking and storing mode, another mode being a data reception/transmitter mode, and also including means enabling received data to be either viewed or heard.

Ex.1002 / Page 273 of 1385
APPLE INC.

FIG.1

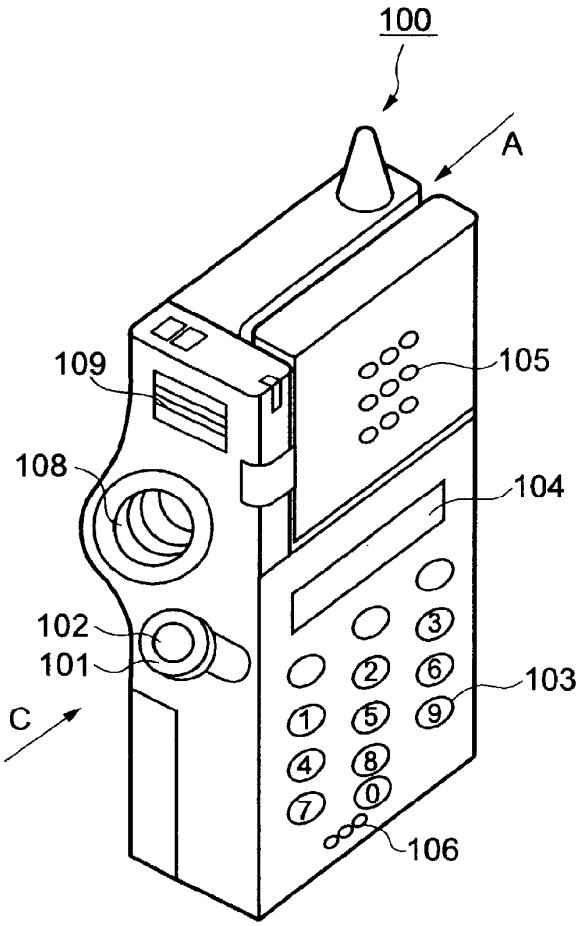


FIG.2

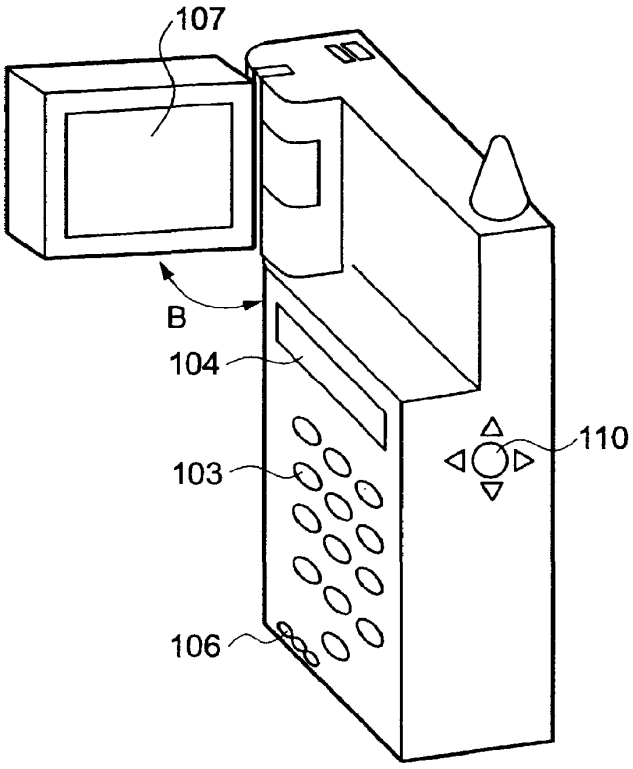


FIG.3

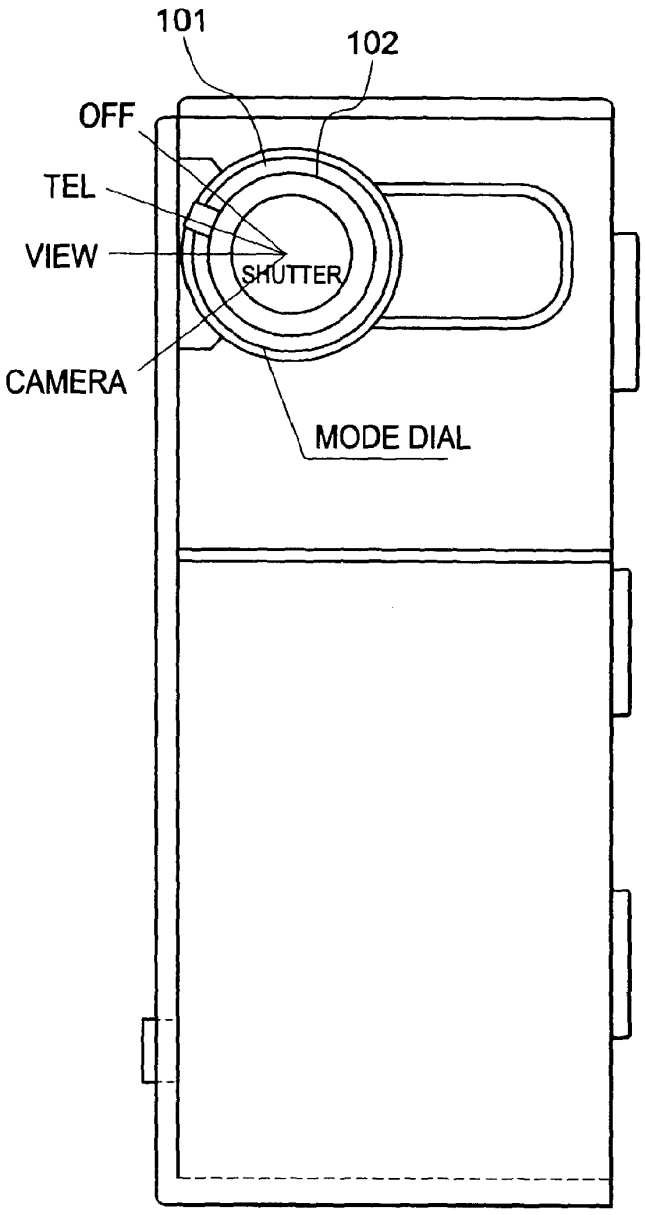


FIG.4

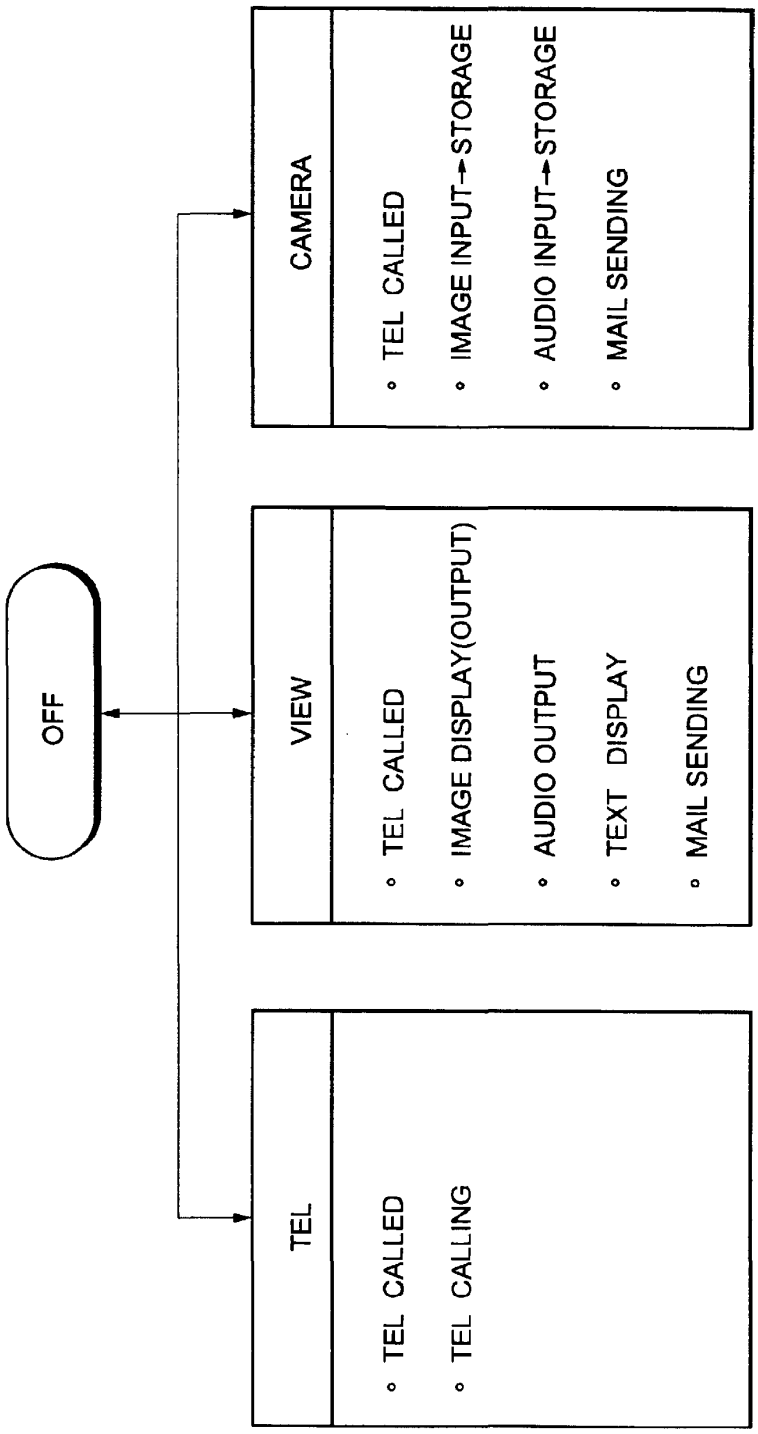
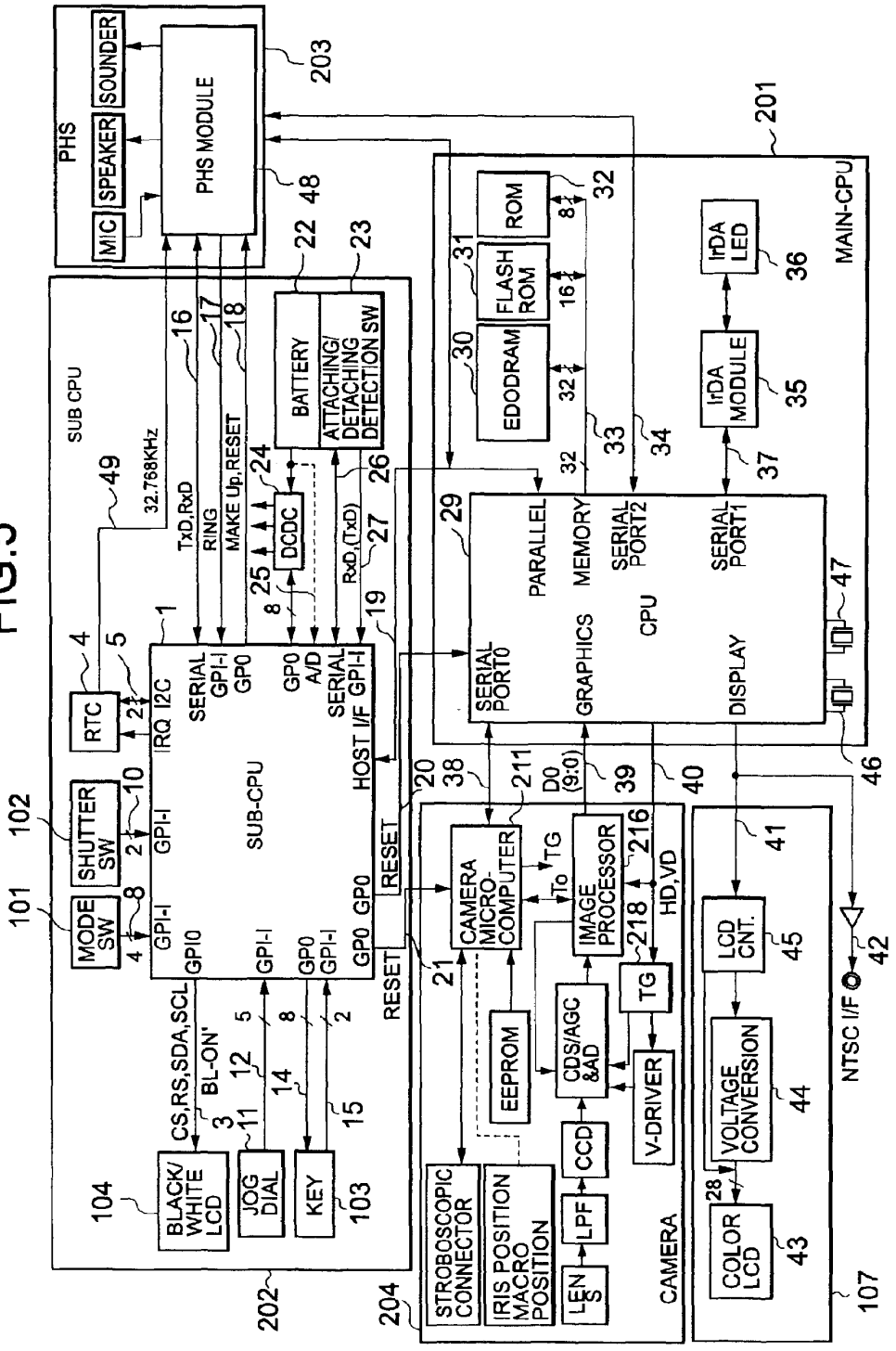

OFF
TEL
TEL CALLED
TEL CALLING
VIEW
TEL CALLED
IMAGE DISPLAY(OUTPUT)
AUDIO OUTPUT
TEXT DISPLAY
MAIL SENDING
CAMERA
TEL CALLED
IMAGE INPUT→STORAGE
AUDIO INPUT→STORAGE
MAIL SENDING

FIG.5



Ex.1002 / Page 278 of 1385
APPLE INC.

FIG.6

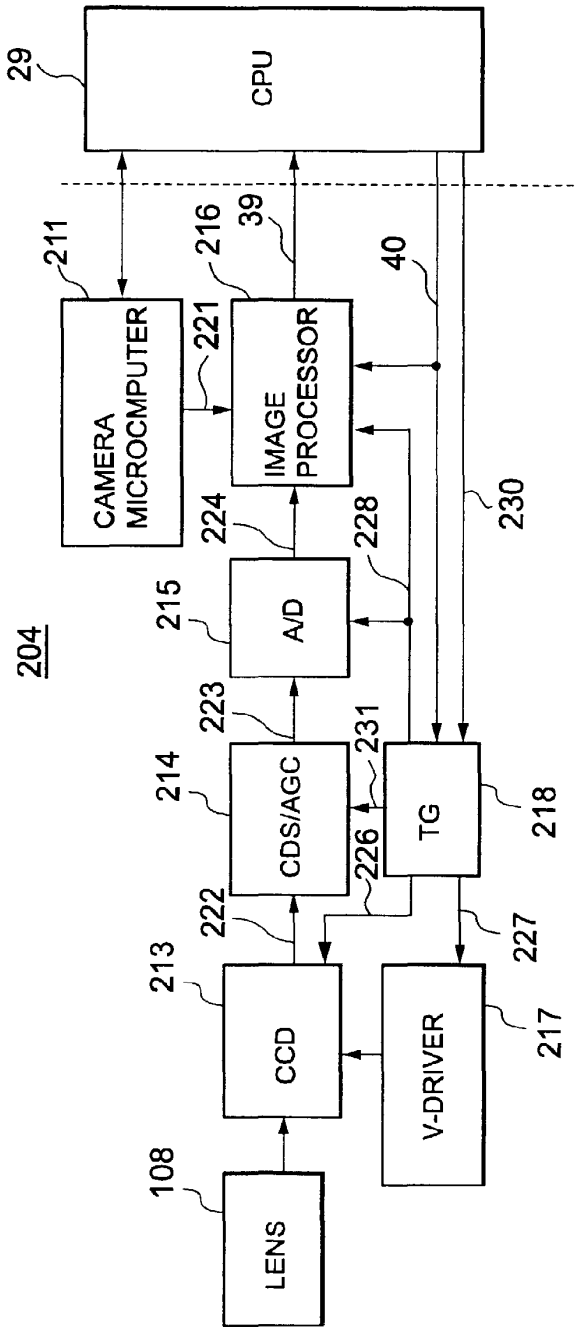

29
CPU
211
216
39
40
CAMERA MICROCMPUTER
221
IMAGE PROCESSOR
224
228
230
204
215
A/D
223
231
214
CDS/AGC
TG
218
226
222
227
213
CCD
V-DRIVER
217
108
LENS

FIG.7

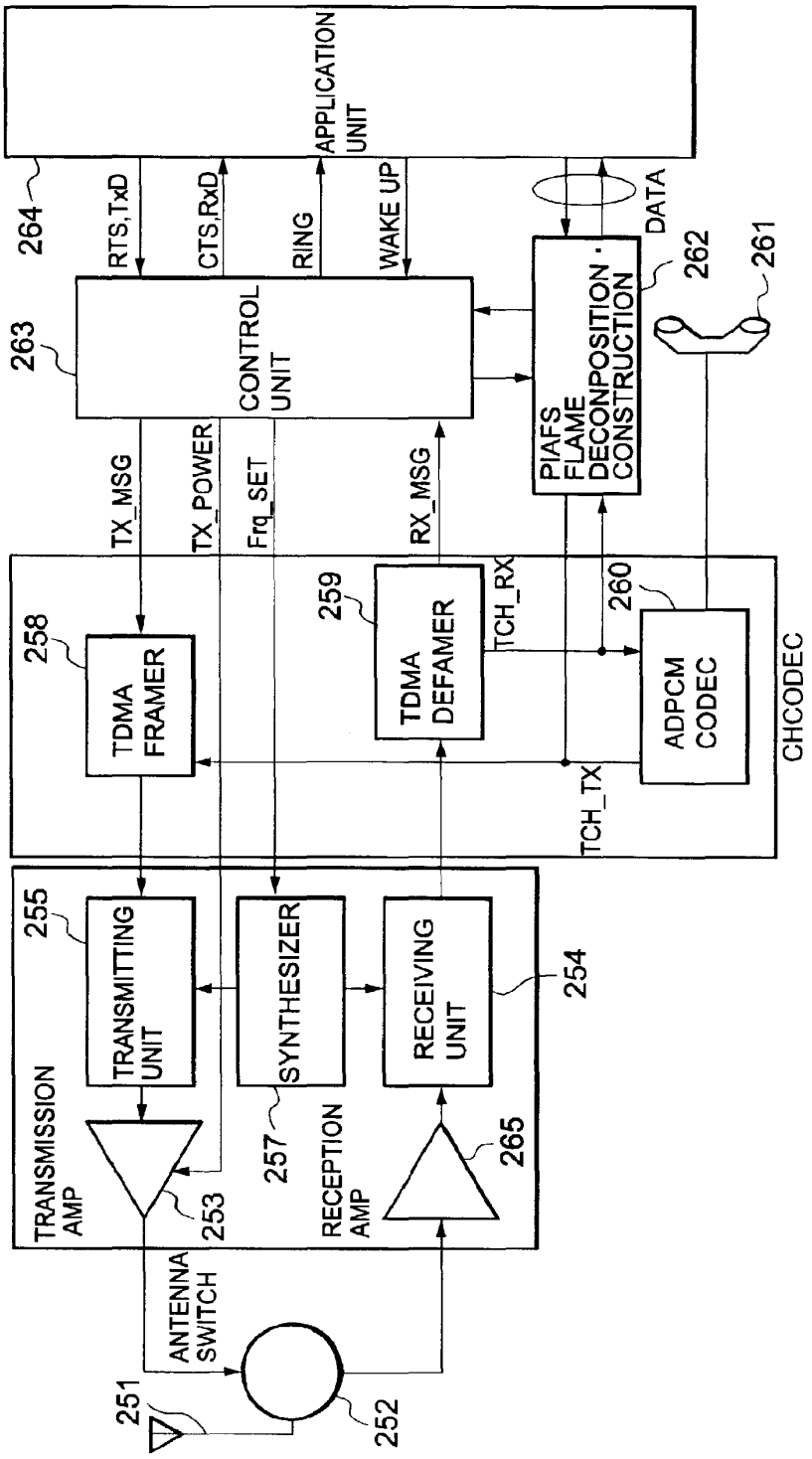

APPLICATION UNIT
264
RTS,TxD
CTS,RxD
RING
WAKE UP
DATA
262
261
263
CONTROL UNIT
PIAFS FLAME DECONPOSITION · CONSTRUCTION
TX_MSG
TX_POWER
Frq_SET
RX_MSG
258
TDMA FRAMER
259
TDMA DEFAMER
TCH_RX
260
ADPCM CODEC
CHCODEC
TCH_TX
255
TRANSMITTING UNIT
SYNTHESIZER
RECEIVING UNIT
254
TRANSMISSION AMP
253
257
RECEPTION AMP
265
ANTENNA SWITCH
251
252

FIG.8

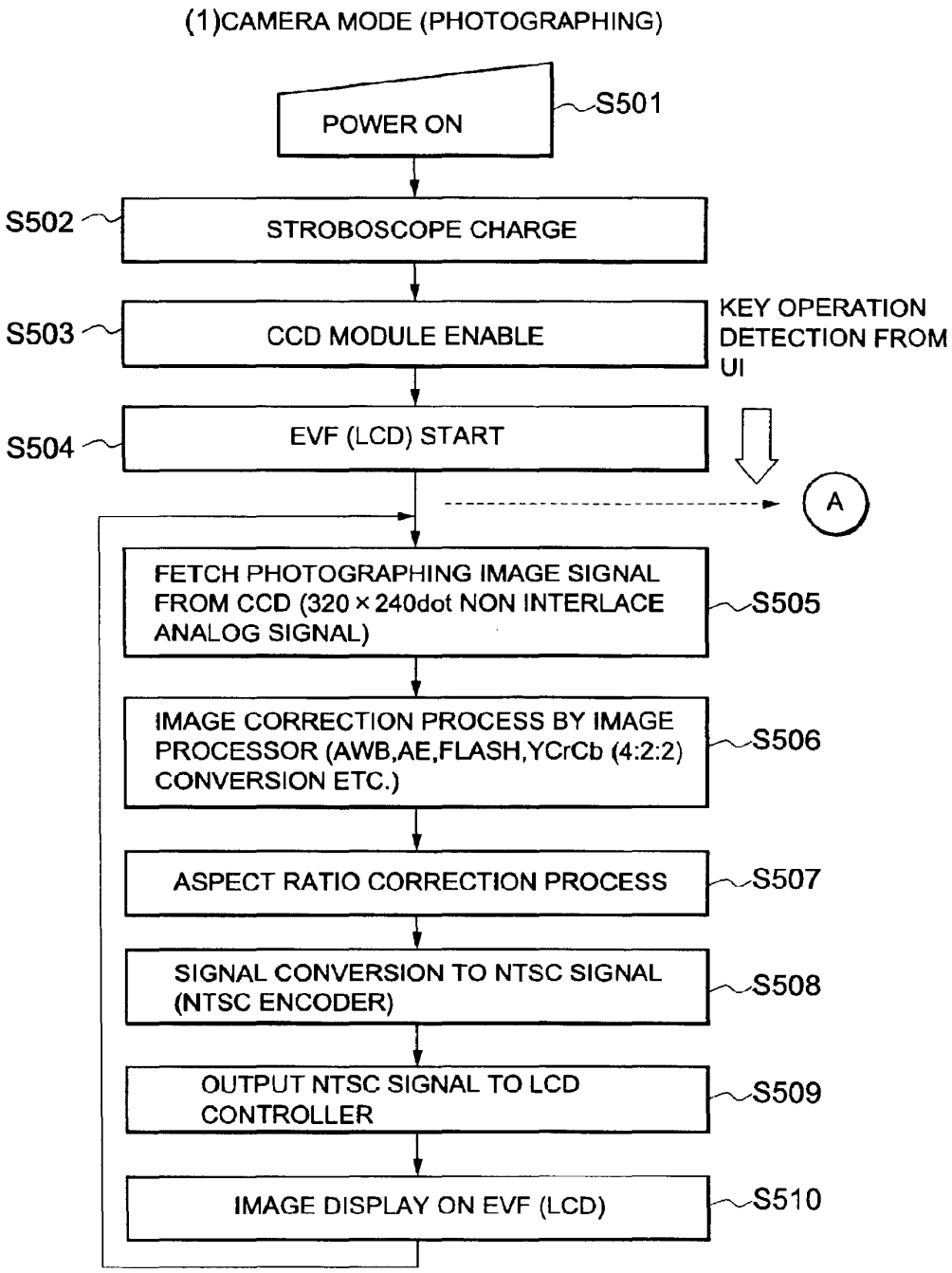

(1)CAMERA MODE (PHOTOGRAPHING)
POWER ON
S501
S502
STROBOSCOPE CHARGE
S503
CCD MODULE ENABLE
KEY OPERATION DETECTION FROM UI
S504
EVF (LCD) START
A
FETCH PHOTOGRAPHING IMAGE SIGNAL FROM CCD (320 × 240dot NON INTERLACE ANALOG SIGNAL)
S505
IMAGE CORRECTION PROCESS BY IMAGE PROCESSOR (AWB,AE,FLASH,YCrCb (4:2:2) CONVERSION ETC.)
S506
ASPECT RATIO CORRECTION PROCESS
S507
SIGNAL CONVERSION TO NTSC SIGNAL (NTSC ENCODER)
S508
OUTPUT NTSC SIGNAL TO LCD CONTROLLER
S509
IMAGE DISPLAY ON EVF (LCD)
S510

FIG.9

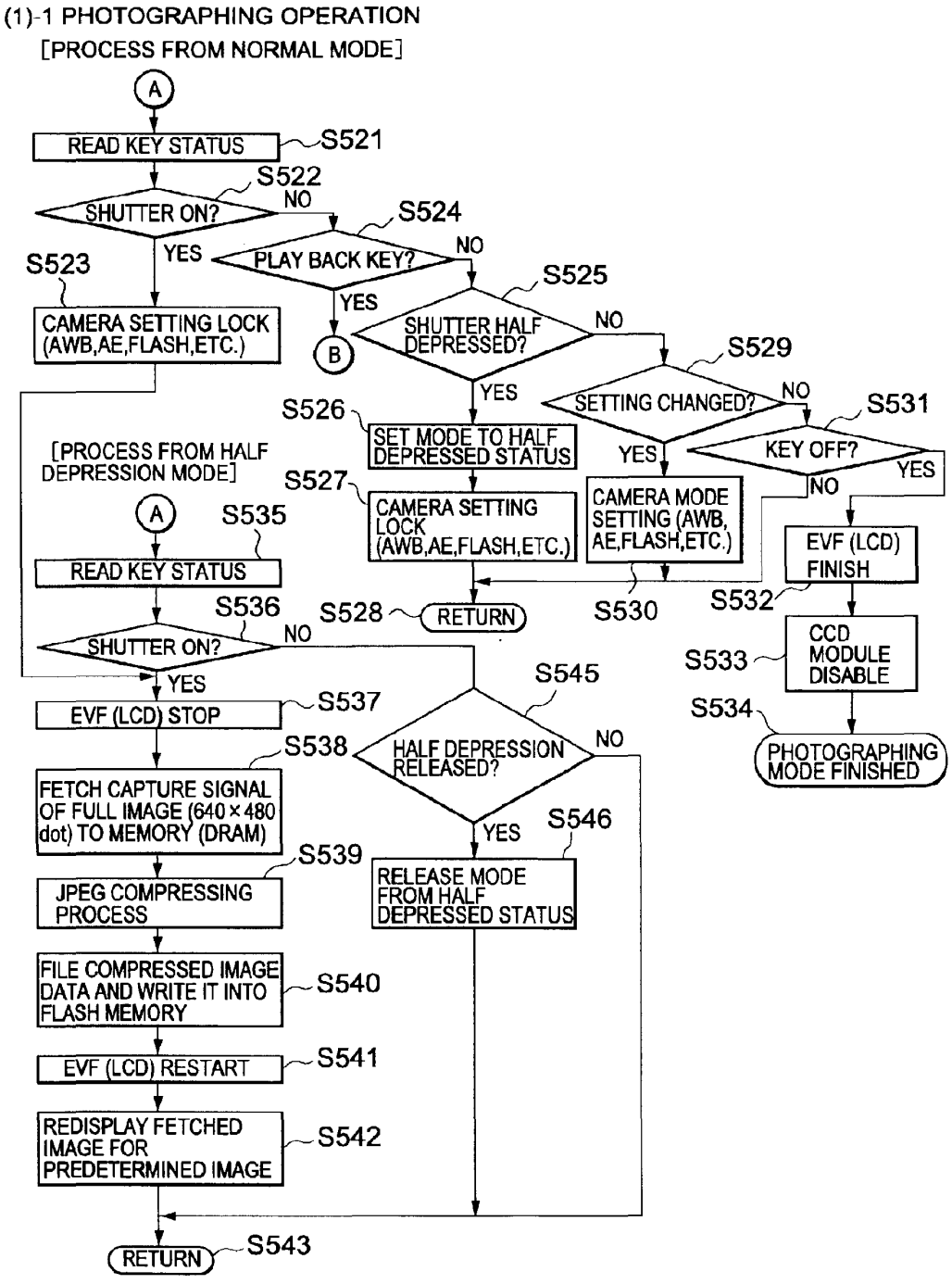

(1)-1 PHOTOGRAPHING OPERATION
[PROCESS FROM NORMAL MODE]
A
READ KEY STATUS
S521
S522
SHUTTER ON?
NO
S524
PLAY BACK KEY?
NO
YES
S523
YES
S525
CAMERA SETTING LOCK (AWB,AE,FLASH,ETC.)
B
SHUTTER HALF DEPRESSED?
NO
S529
YES
SETTING CHANGED?
NO
S531
S526
SET MODE TO HALF DEPRESSED STATUS
YES
KEY OFF?
YES
[PROCESS FROM HALF DEPRESSION MODE]
S527
NO
A
S535
CAMERA SETTING LOCK (AWB,AE,FLASH,ETC.)
CAMERA MODE SETTING (AWB, AE,FLASH,ETC.)
EVF (LCD) FINISH
READ KEY STATUS
S536
S528
RETURN
S530
S532
SHUTTER ON?
NO
CCD MODULE DISABLE
S533
YES
S545
S534
EVF (LCD) STOP
S537
HALF DEPRESSION RELEASED?
NO
PHOTOGRAPHING MODE FINISHED
S538
YES
S546
FETCH CAPTURE SIGNAL OF FULL IMAGE (640×480 dot) TO MEMORY (DRAM)
S539
RELEASE MODE FROM HALF DEPRESSED STATUS
JPEG COMPRESSING PROCESS
FILE COMPRESSED IMAGE DATA AND WRITE IT INTO FLASH MEMORY
S540
EVF (LCD) RESTART
S541
REDISPLAY FETCHED IMAGE FOR PREDETERMINED IMAGE
S542
RETURN
S543

FIG.10

(1)-2 PLAY BACK OPERATION

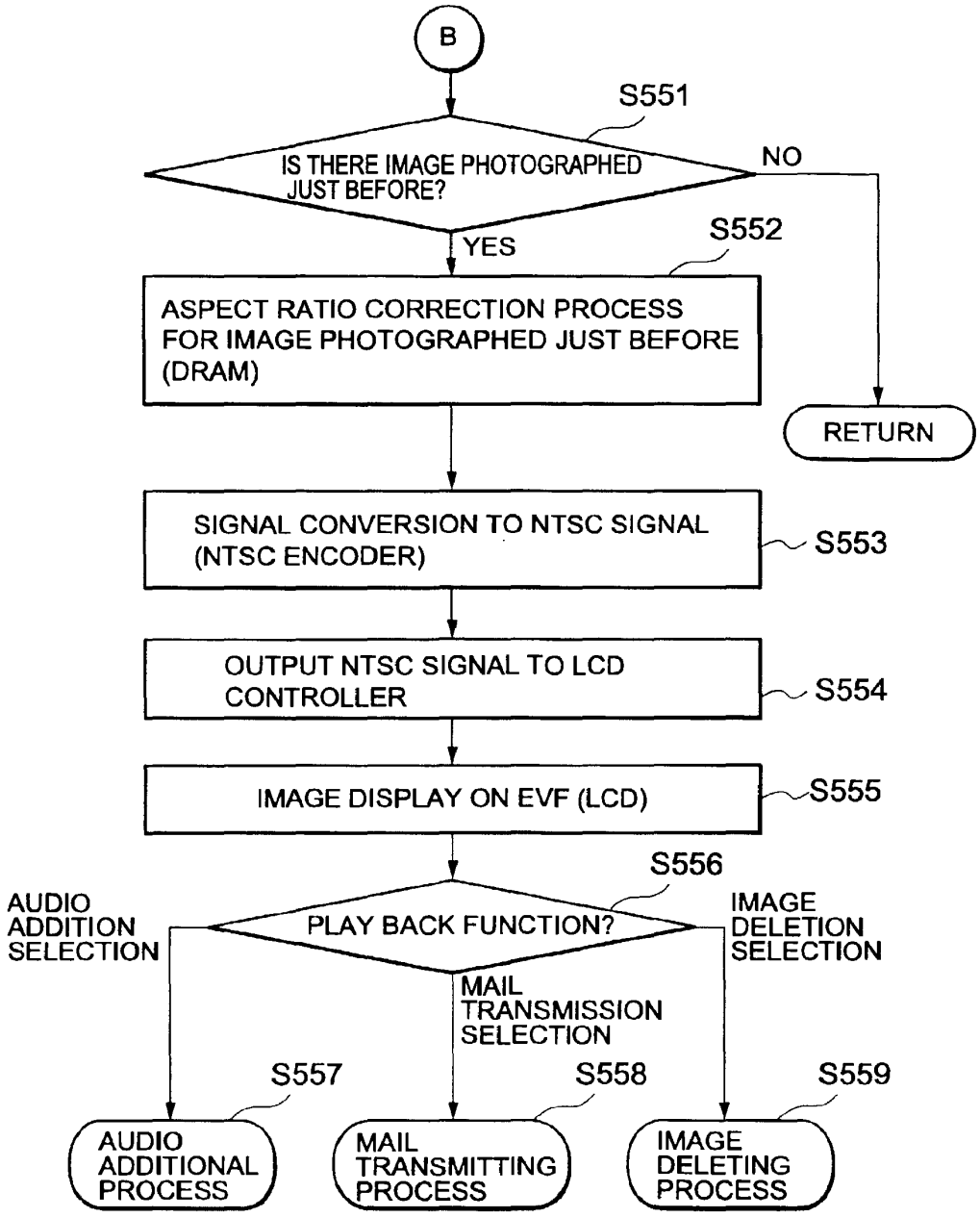


FIG.11

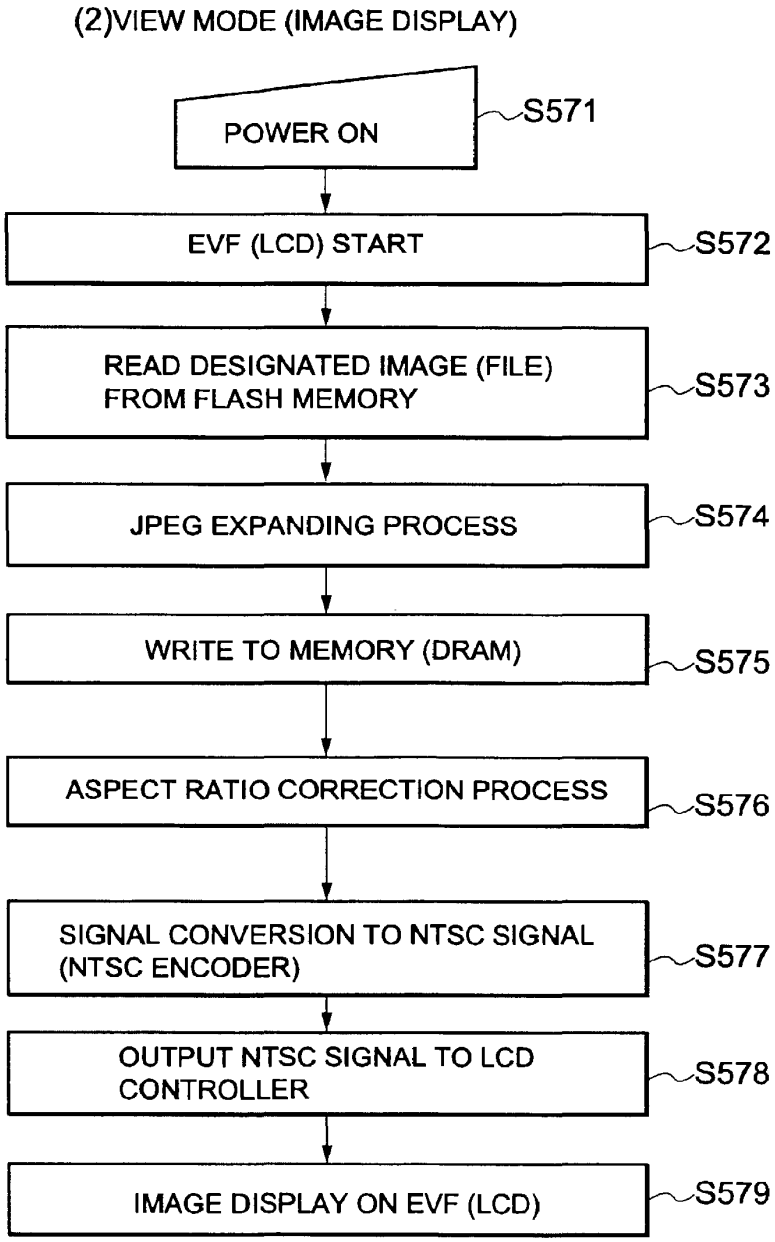
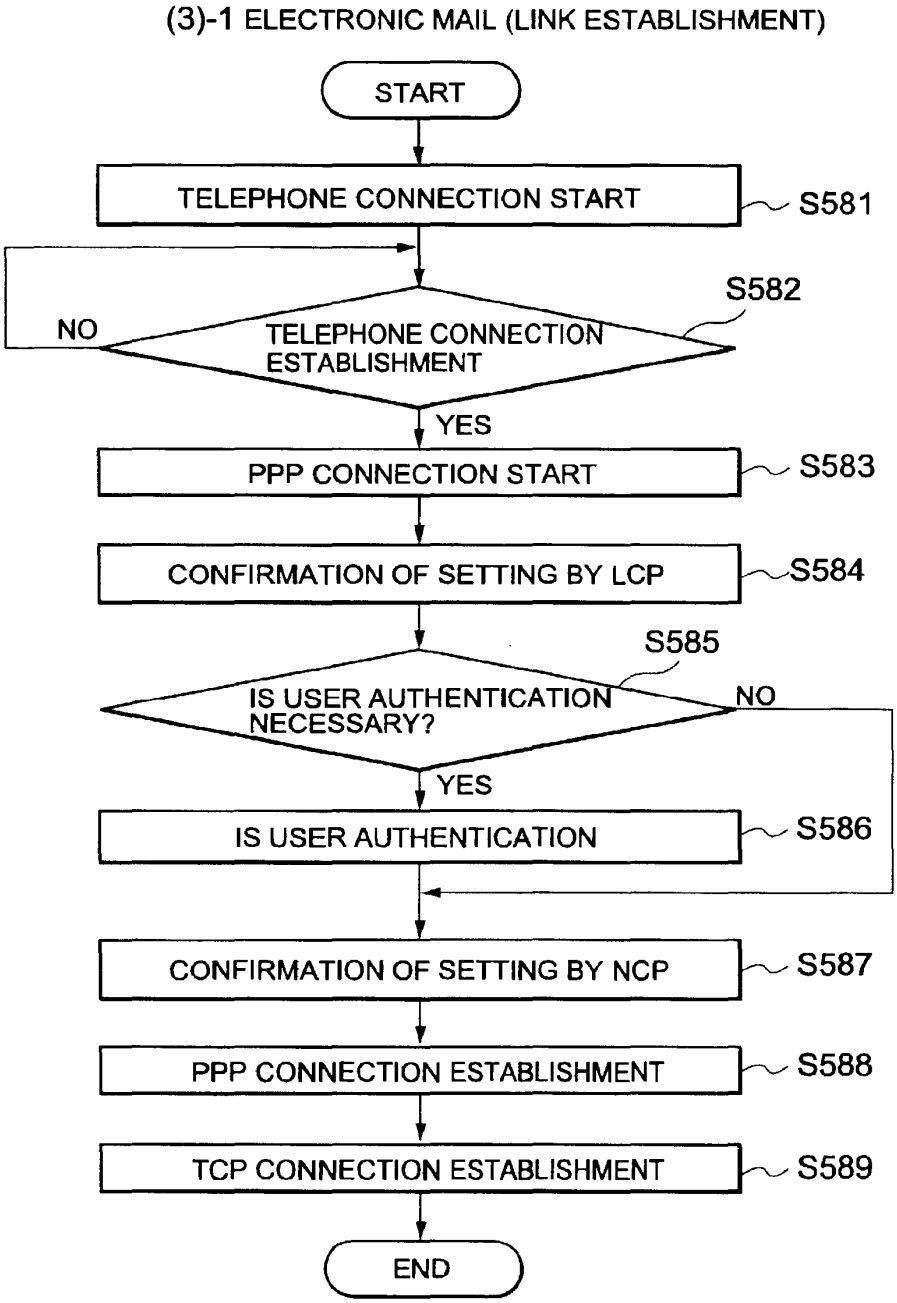

(2)VIEW MODE (IMAGE DISPLAY)
POWER ON
S571
EVF (LCD) START
S572
READ DESIGNATED IMAGE (FILE) FROM FLASH MEMORY
S573
JPEG EXPANDING PROCESS
S574
WRITE TO MEMORY (DRAM)
S575
ASPECT RATIO CORRECTION PROCESS
S576
SIGNAL CONVERSION TO NTSC SIGNAL (NTSC ENCODER)
S577
OUTPUT NTSC SIGNAL TO LCD CONTROLLER
S578
IMAGE DISPLAY ON EVF (LCD)
S579

FIG.12



Ex.1002 / Page 285 of 1385
APPLE INC.

FIG.13

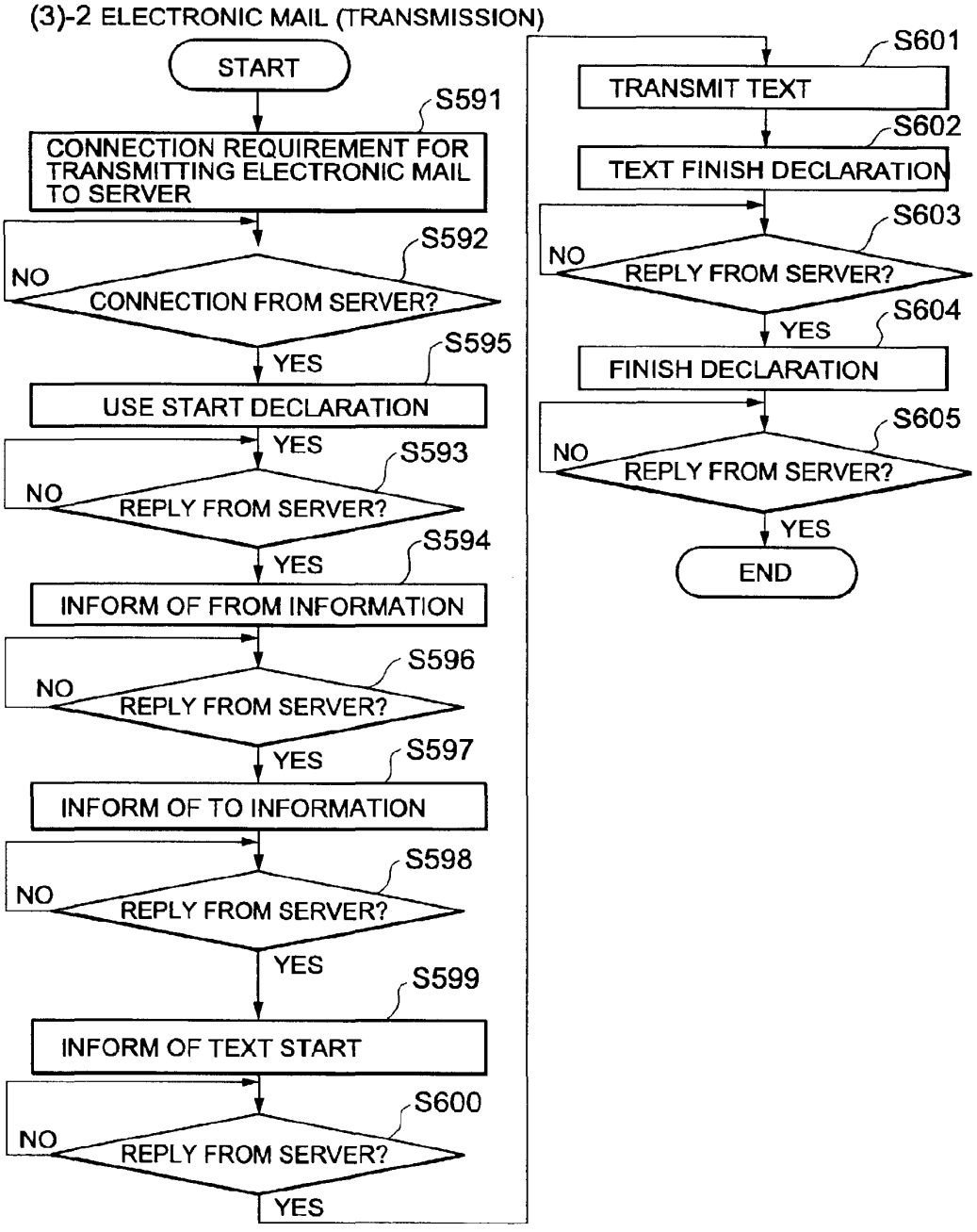
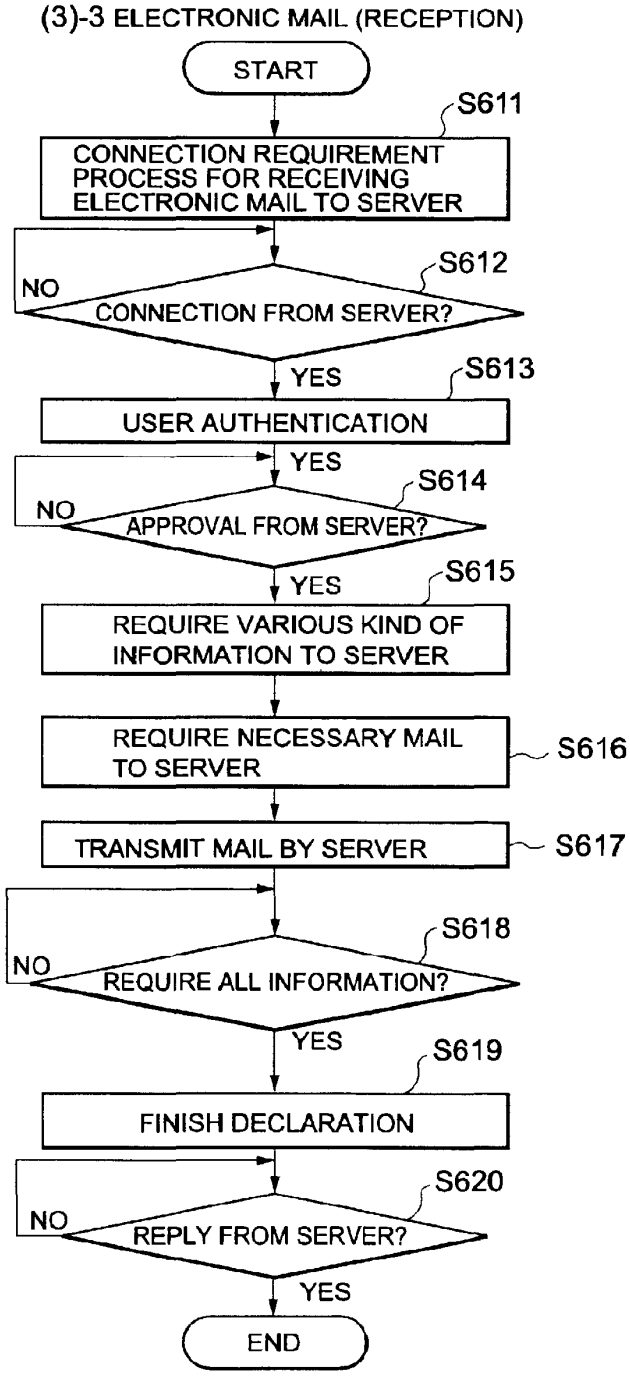

(3)-2 ELECTRONIC MAIL (TRANSMISSION)
START
S591
CONNECTION REQUIREMENT FOR TRANSMITTING ELECTRONIC MAIL TO SERVER
S592
NO
CONNECTION FROM SERVER?
YES
S595
USE START DECLARATION
YES
S593
NO
REPLY FROM SERVER?
YES
S594
INFORM OF FROM INFORMATION
S596
NO
REPLY FROM SERVER?
YES
S597
INFORM OF TO INFORMATION
S598
NO
REPLY FROM SERVER?
YES
S599
INFORM OF TEXT START
S600
NO
REPLY FROM SERVER?
YES
S601
TRANSMIT TEXT
S602
TEXT FINISH DECLARATION
S603
NO
REPLY FROM SERVER?
YES
S604
FINISH DECLARATION
S605
NO
REPLY FROM SERVER?
YES
END

FIG.14



Ex.1002 / Page 287 of 1385
APPLE INC.

FIG.15

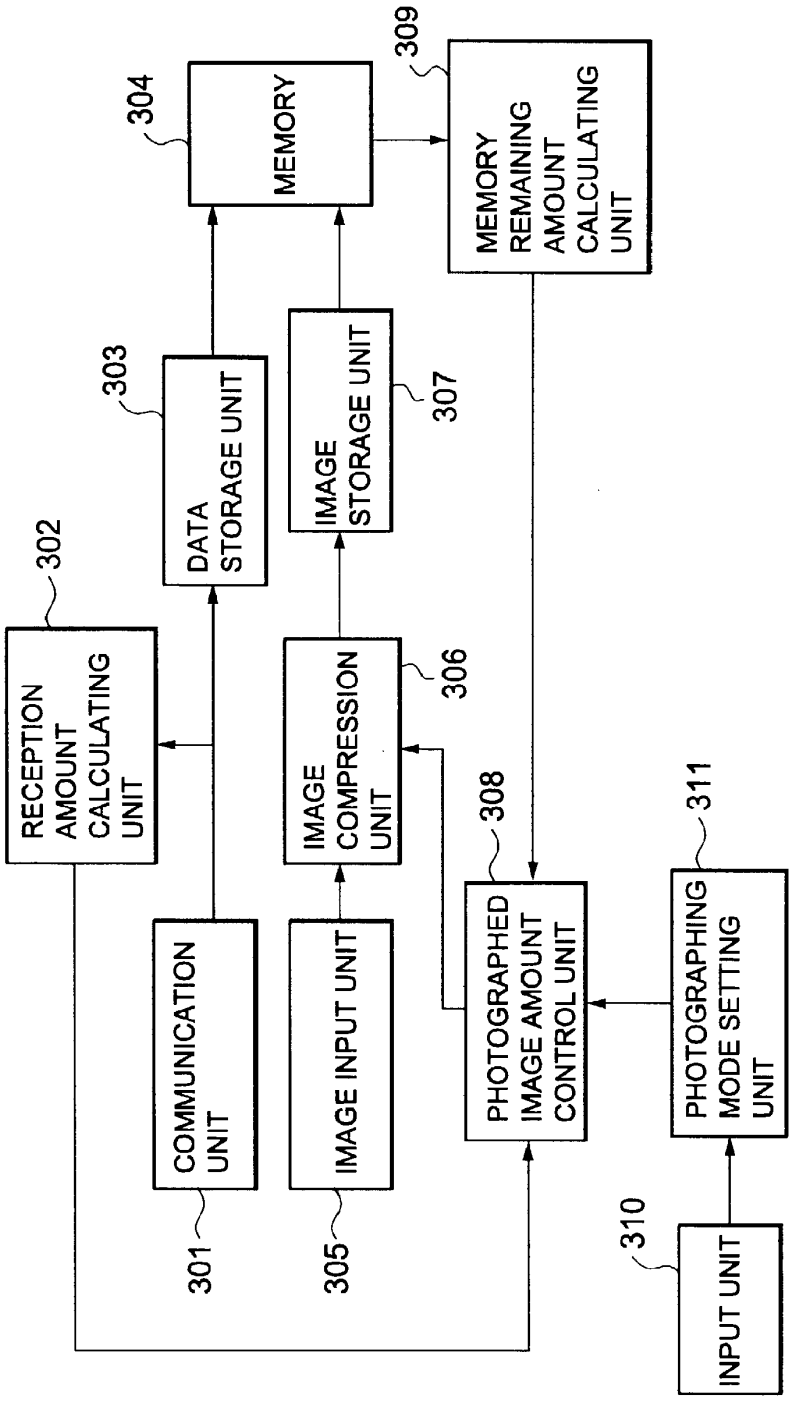

309
304
MEMORY
MEMORY REMAINING AMOUNT CALCULATING UNIT
303
DATA STORAGE UNIT
IMAGE STORAGE UNIT
307
302
RECEPTION AMOUNT CALCULATING UNIT
IMAGE COMPRESSION UNIT
306
308
311
COMMUNICATION UNIT
IMAGE INPUT UNIT
PHOTOGRAPHED IMAGE AMOUNT CONTROL UNIT
PHOTOGRAPHING MODE SETTING UNIT
301
305
310
INPUT UNIT

FIG.16

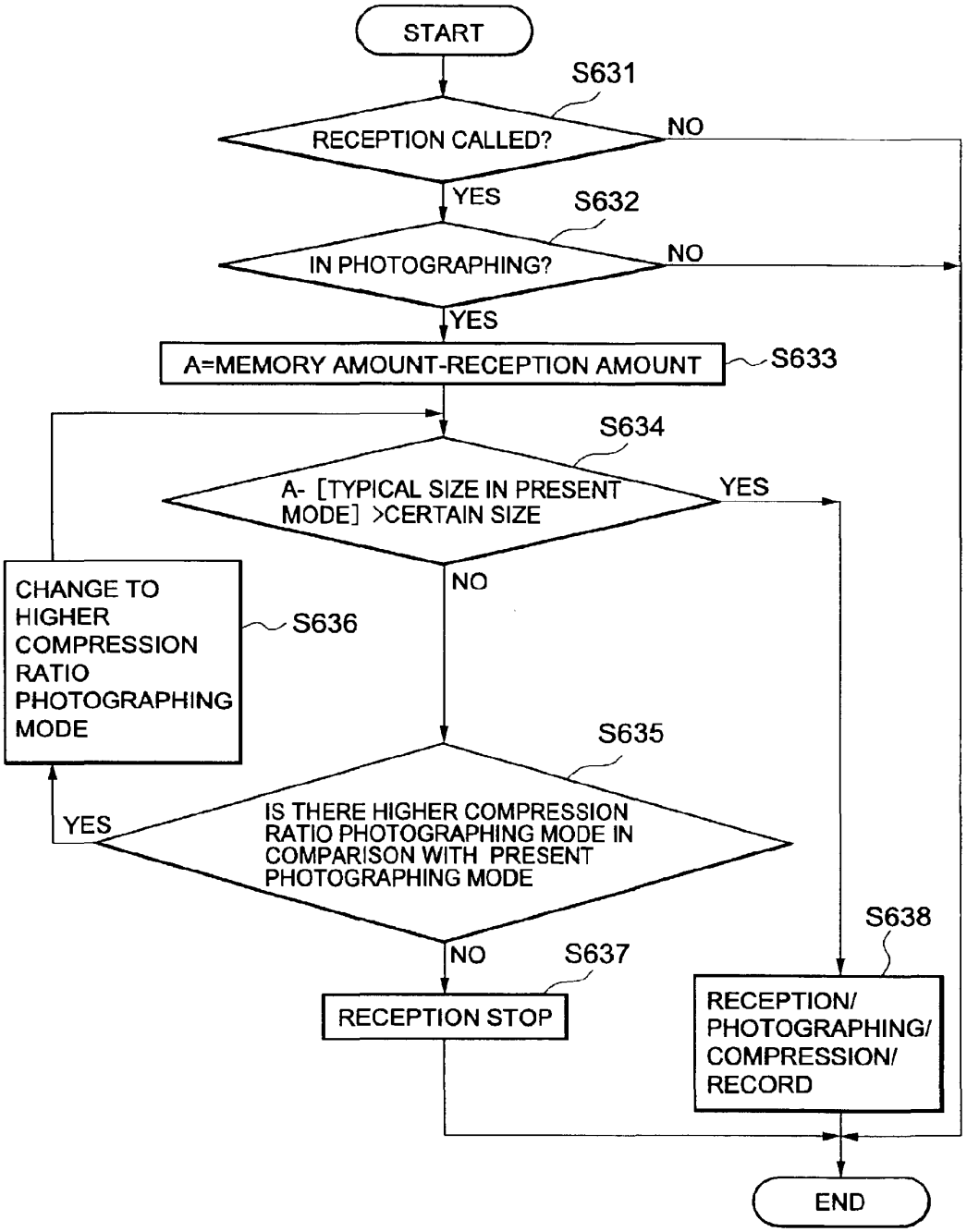

START
S631
RECEPTION CALLED?
NO
YES
S632
IN PHOTOGRAPHING?
NO
YES
A=MEMORY AMOUNT-RECEPTION AMOUNT
S633
S634
A- [TYPICAL SIZE IN PRESENT MODE] >CERTAIN SIZE
YES
NO
CHANGE TO HIGHER COMPRESSION RATIO PHOTOGRAPHING MODE
S636
S635
YES
IS THERE HIGHER COMPRESSION RATIO PHOTOGRAPHING MODE IN COMPARISON WITH PRESENT PHOTOGRAPHING MODE
S638
NO
S637
RECEPTION STOP
RECEPTION/ PHOTOGRAPHING/ COMPRESSION/ RECORD
END

FIG.17

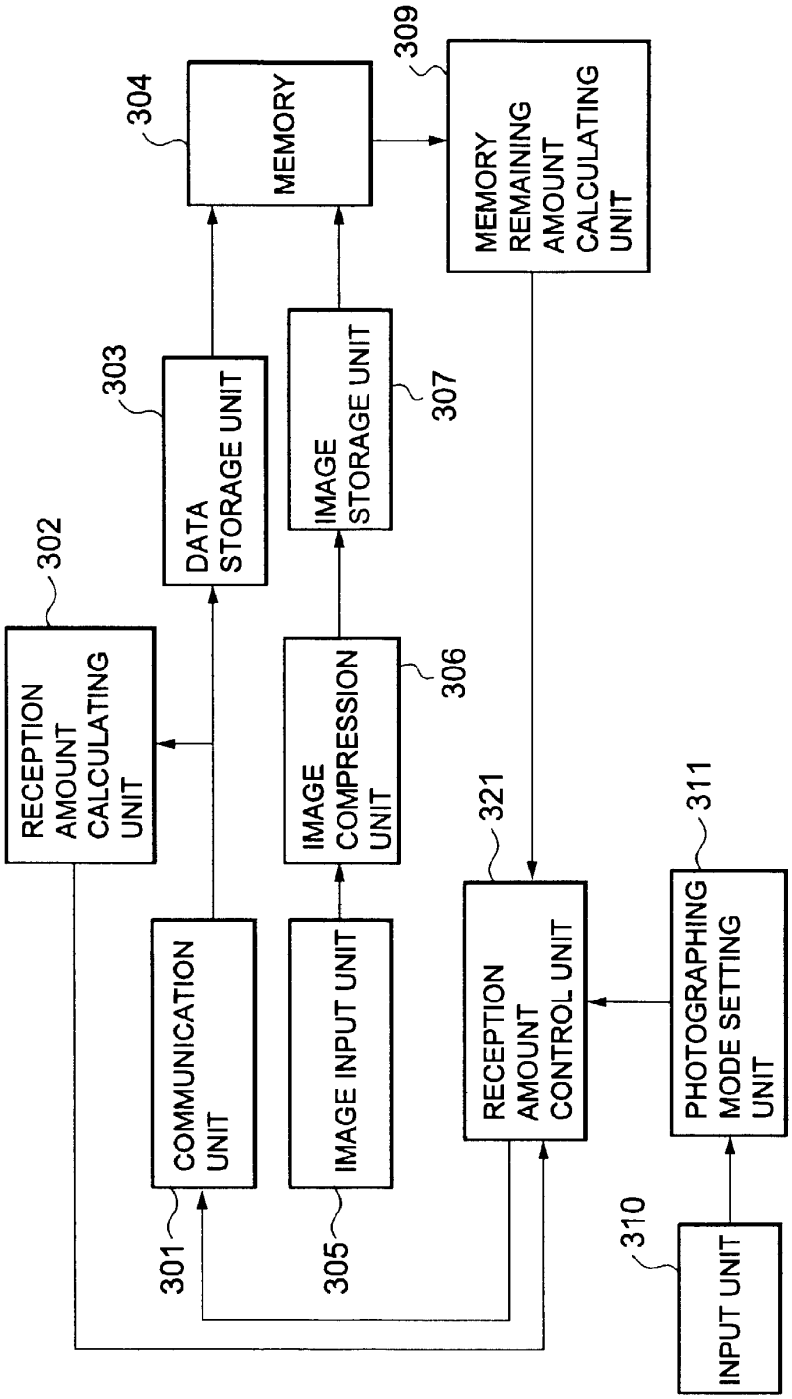

304
MEMORY
309
MEMORY REMAINING AMOUNT CALCULATING UNIT
303
DATA STORAGE UNIT
307
IMAGE STORAGE UNIT
302
RECEPTION AMOUNT CALCULATING UNIT
306
IMAGE COMPRESSION UNIT
321
311
COMMUNICATION UNIT
IMAGE INPUT UNIT
RECEPTION AMOUNT CONTROL UNIT
PHOTOGRAPHING MODE SETTING UNIT
301
305
310
INPUT UNIT

FIG.18

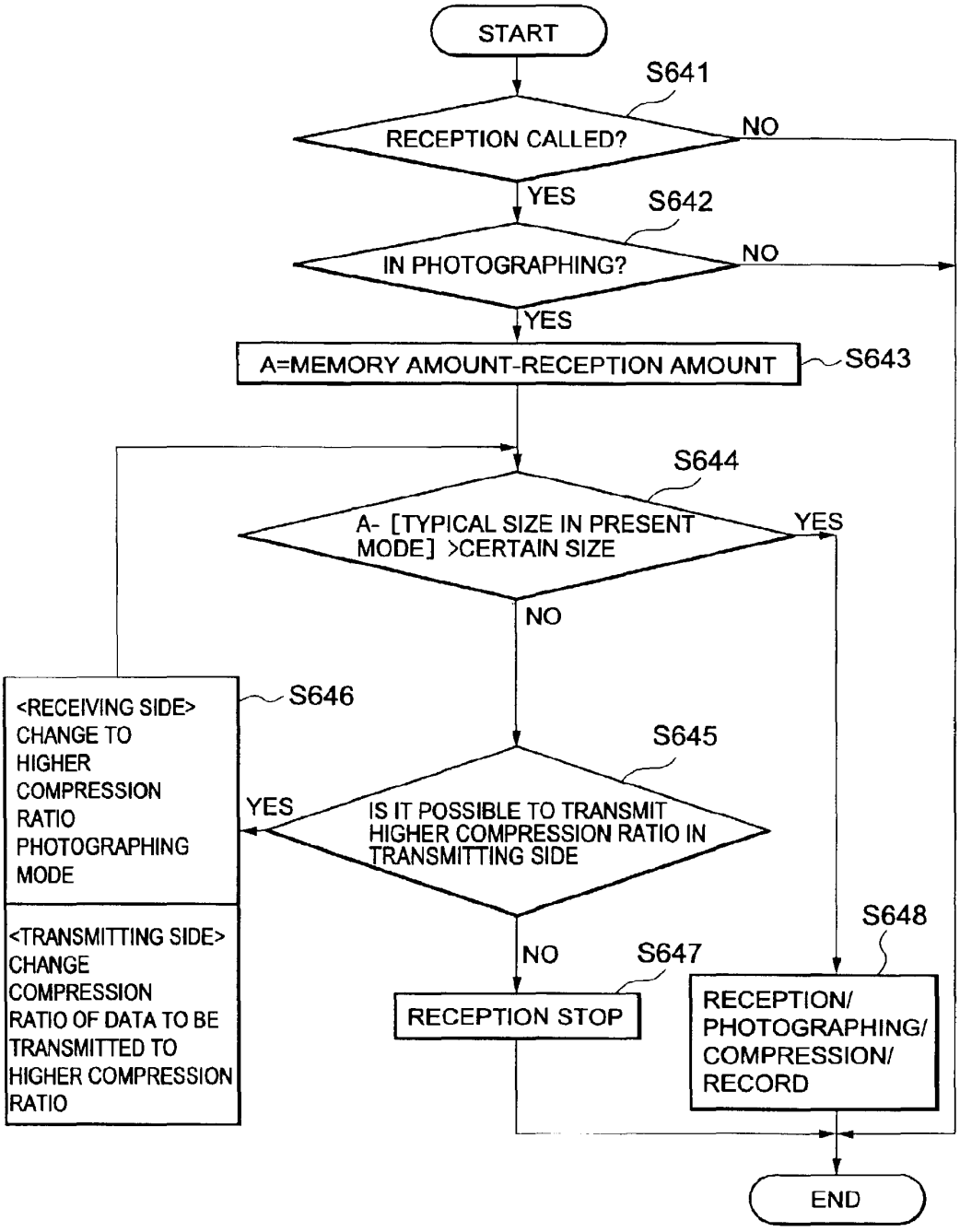

START
S641
RECEPTION CALLED?
NO
YES
S642
IN PHOTOGRAPHING?
NO
YES
A=MEMORY AMOUNT-RECEPTION AMOUNT
S643
S644
A- [TYPICAL SIZE IN PRESENT MODE] >CERTAIN SIZE
YES
NO
<RECEIVING SIDE> CHANGE TO HIGHER COMPRESSION RATIO PHOTOGRAPHING MODE
S646
S645
YES
IS IT POSSIBLE TO TRANSMIT HIGHER COMPRESSION RATIO IN TRANSMITTING SIDE
<TRANSMITTING SIDE> CHANGE COMPRESSION RATIO OF DATA TO BE TRANSMITTED TO HIGHER COMPRESSION RATIO
NO
S647
RECEPTION STOP
S648
RECEPTION/ PHOTOGRAPHING/ COMPRESSION/ RECORD
END

FIG.19

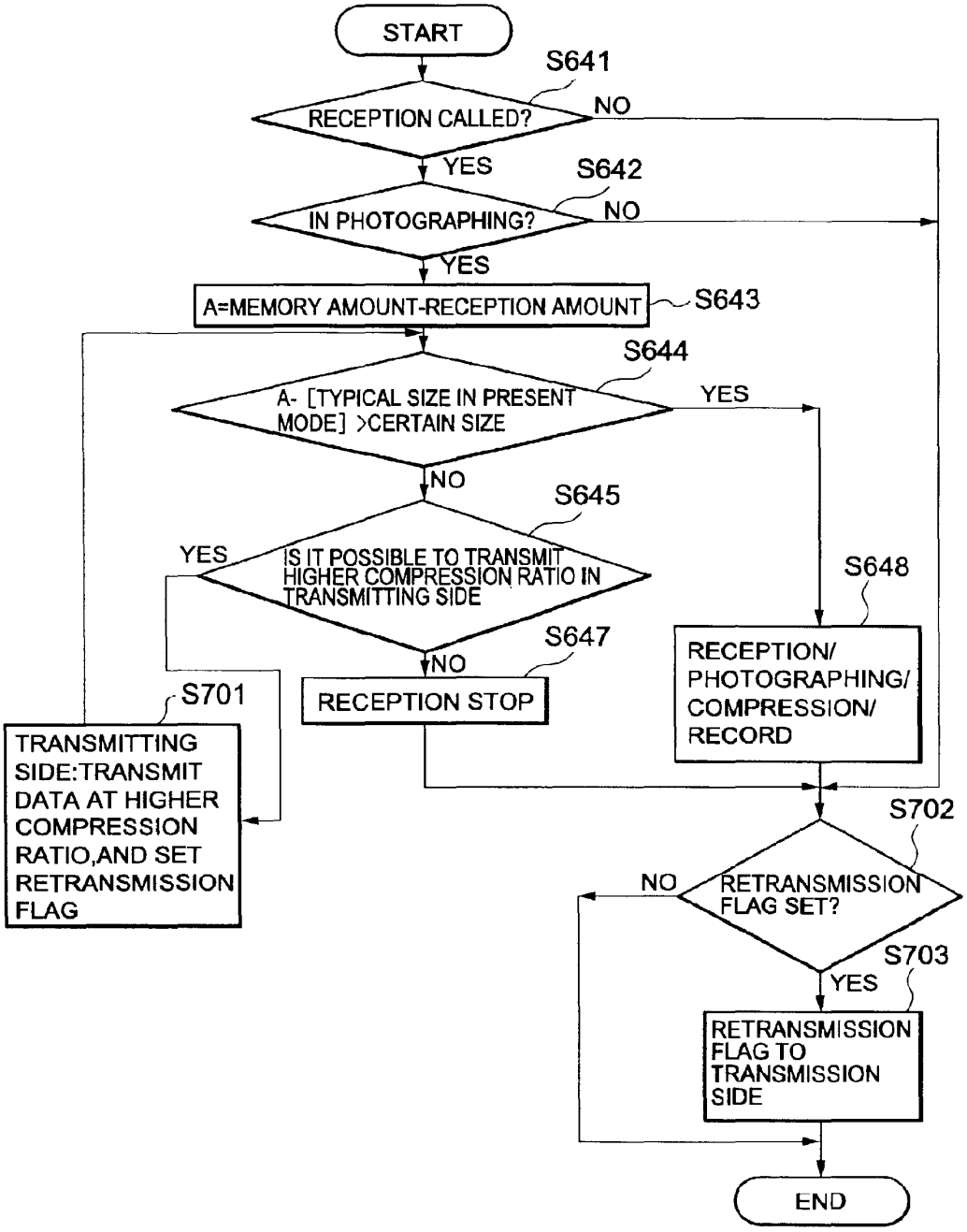

START
S641
RECEPTION CALLED?
NO
YES
S642
IN PHOTOGRAPHING?
NO
YES
A=MEMORY AMOUNT-RECEPTION AMOUNT
S643
S644
A- [TYPICAL SIZE IN PRESENT MODE] >CERTAIN SIZE
YES
NO
S645
YES
IS IT POSSIBLE TO TRANSMIT HIGHER COMPRESSION RATIO IN TRANSMITTING SIDE
S648
S647
NO
RECEPTION STOP
RECEPTION/ PHOTOGRAPHING/ COMPRESSION/ RECORD
S701
TRANSMITTING SIDE:TRANSMIT DATA AT HIGHER COMPRESSION RATIO,AND SET RETRANSMISSION FLAG
S702
NO
RETRANSMISSION FLAG SET?
S703
YES
RETRANSMISSION FLAG TO TRANSMISSION SIDE
END

FIG.20

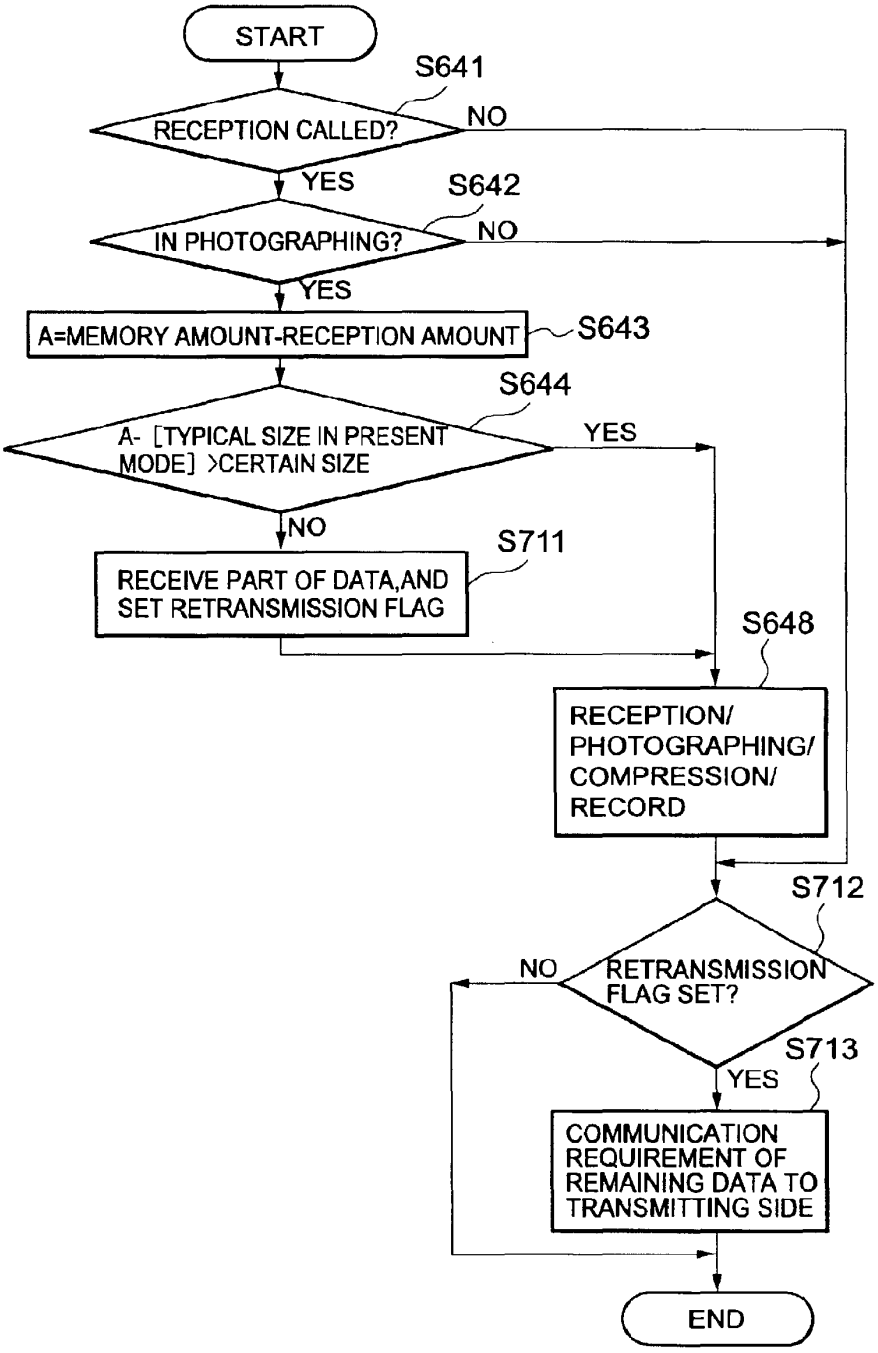

START
S641
RECEPTION CALLED?
NO
YES
S642
IN PHOTOGRAPHING?
NO
YES
A=MEMORY AMOUNT-RECEPTION AMOUNT
S643
S644
A- [TYPICAL SIZE IN PRESENT MODE] >CERTAIN SIZE
YES
NO
S711
RECEIVE PART OF DATA,AND SET RETRANSMISSION FLAG
S648
RECEPTION/ PHOTOGRAPHING/ COMPRESSION/ RECORD
S712
NO
RETRANSMISSION FLAG SET?
S713
YES
COMMUNICATION REQUIREMENT OF REMAINING DATA TO TRANSMITTING SIDE
END

FIG.21

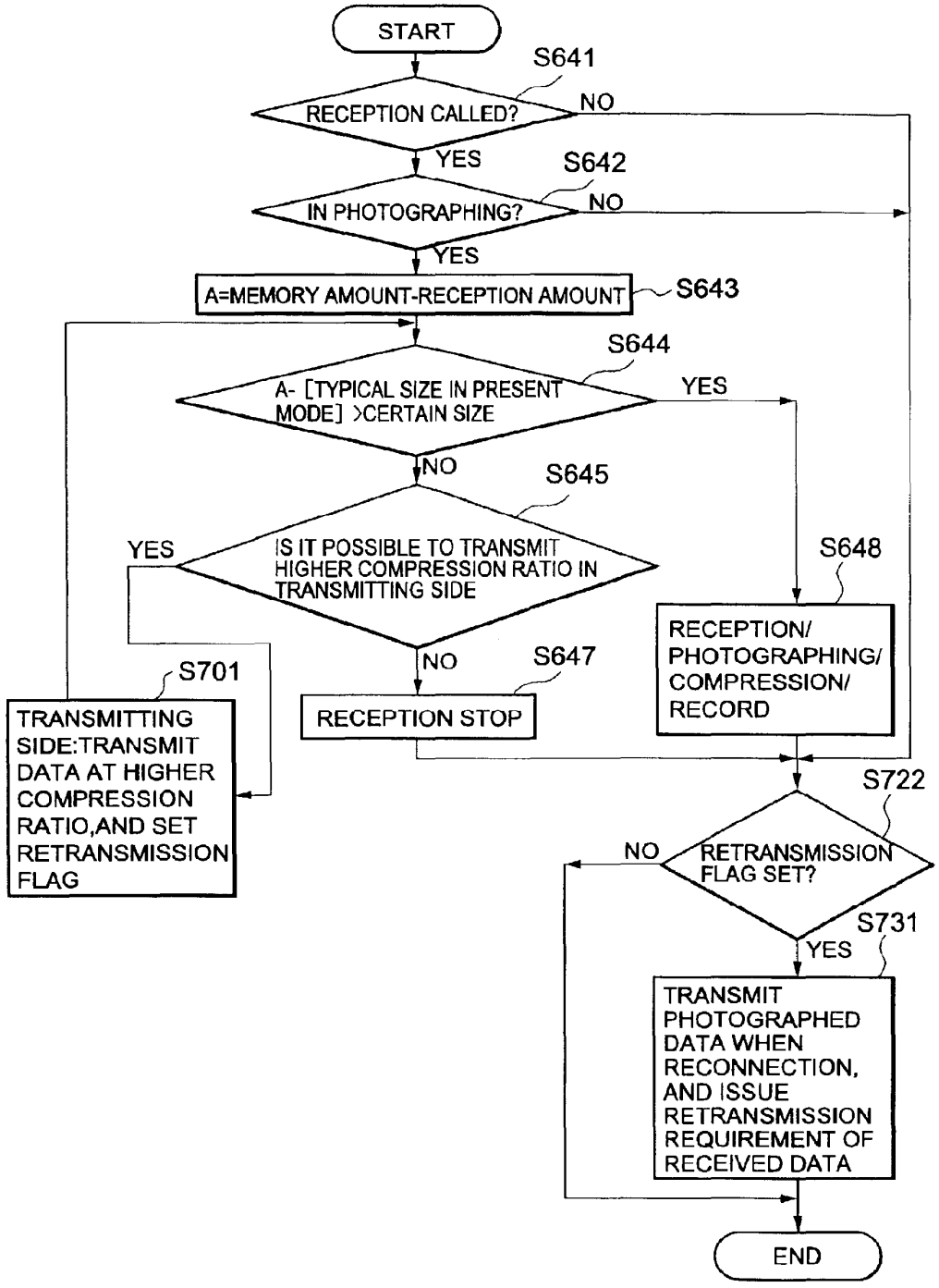
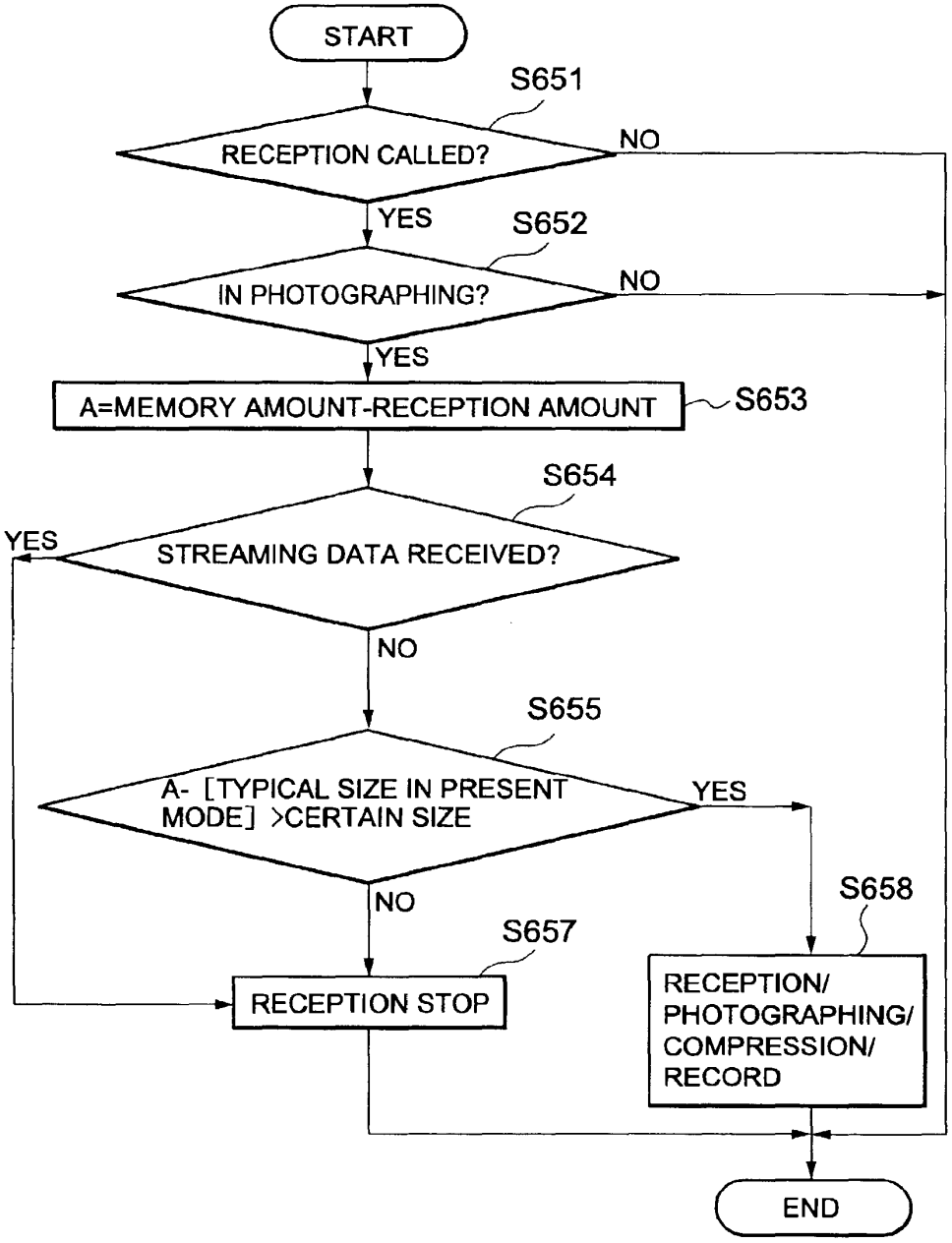

START
S641
RECEPTION CALLED?
NO
YES
S642
IN PHOTOGRAPHING?
NO
YES
A=MEMORY AMOUNT-RECEPTION AMOUNT
S643
S644
A- [TYPICAL SIZE IN PRESENT MODE] >CERTAIN SIZE
YES
NO
S645
IS IT POSSIBLE TO TRANSMIT HIGHER COMPRESSION RATIO IN TRANSMITTING SIDE
YES
NO
S647
RECEPTION STOP
S648
RECEPTION/ PHOTOGRAPHING/ COMPRESSION/ RECORD
S701
TRANSMITTING SIDE:TRANSMIT DATA AT HIGHER COMPRESSION RATIO,AND SET RETRANSMISSION FLAG
S722
NO
RETRANSMISSION FLAG SET?
S731
YES
TRANSMIT PHOTOGRAPHED DATA WHEN RECONNECTION, AND ISSUE RETRANSMISSION REQUIREMENT OF RECEIVED DATA
END

FIG.22


START
S651
RECEPTION CALLED?
NO
YES
S652
IN PHOTOGRAPHING?
NO
YES
A=MEMORY AMOUNT-RECEPTION AMOUNT
S653
S654
STREAMING DATA RECEIVED?
YES
NO
S655
A- [TYPICAL SIZE IN PRESENT MODE] >CERTAIN SIZE
YES
NO
S658
S657
RECEPTION STOP
RECEPTION/ PHOTOGRAPHING/ COMPRESSION/ RECORD
END

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 July 2001 (19.07.2001)

PCT

(10) International Publication Number
WO 01/52178 A1

(51) International Patent Classification[7]: G06K 9/00

(21) International Application Number: PCT/US01/01043

(22) International Filing Date: 11 January 2001 (11.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/482,786	13 January 2000 (13.01.2000)	US
09/507,096	17 February 2000 (17.02.2000)	US
60/198,857	21 April 2000 (21.04.2000)	US

(71) Applicant *(for all designated States except US)*: **DIGIMARC CORPORATION** [US/US]; 19801 SW 72nd Avenue, Suite 250, Tualatin, OR 97062 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DAVIS, Bruce, L.** [US/US]; 15599 Village Drive, Lake Oswego, OR 97034 (US). **RHOADS, Geoffrey, B.** [US/US]; 2961 SW Turner Road, West Linn, OR 97068 (US). **CONWELL, William, Y.** [US/US]; 6224 S.W. Tower Way, Portland, OR 97221 (US).

(74) Agent: **MEYER, Joel, R.**; Digimarc Corporation, 19801 S.W. 72nd Avenue, Suite 250, Tualatin, OR 97062 (US).

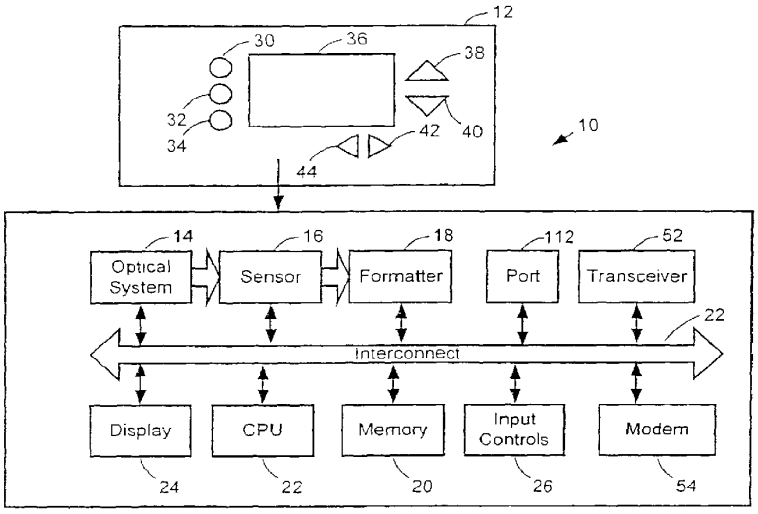
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: AUTHENTICATING METADATA AND EMBEDDING METADATA IN WATERMARKS OF MEDIA SIGNALS



(57) Abstract: A steganographic embedder associates data with a media signal by encoding the data, a link to the data, or a combination of both into the media signal. The embedder may be located in a media signal capture device or an external process or device (Fig. 2, 100). In one application, for example, an embedder process steganographically encodes data into a media signal as part of the process of uploading the media signal from the media signal capture device to an external device (Fig. 2, 106). In another applications, a media signal capture device includes a steganographic embedder that encodes data or a link to external metadata into the media signal at the time of recording (Fig. 3).

WO 01/52178 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Authenticating Metadata and Embedding Metadata in Watermarks of Media Signals

Field of the Invention

The invention relates to encoding and authenticating data associated with media signal objects like images, audio, computer generated graphics, video, etc.

Background and Summary of the Invention

Conventional still image and movie cameras memorialized image data on media (e.g., film or magnetic tape), but did not include provision to store other useful information.

Some years ago, still-image cameras with the capability to insert visible date text in a corner of the image frame became available, solving the problem of trying to recall the dates that photos of interest were taken.

More recently, the Advanced Photo System provided a magnetic encoding medium on the back of photographic film, permitting additional information to be stored (e.g., exposure information, whether flash was used, desired print size, etc.).

With the growing popularity of digital storage of image data, it would be helpful if auxiliary data could be stored in association with a photo. Such storage is now possible in the header fields of certain popular data formats, but such data can be lost if the file is converted to another format.

Considering broader multimedia applications, it is useful to associate data (metadata) with media signals such as audio, video, computer generated graphics models, and still images. Some examples include associating the owner of an image with the image, or associating a picture with a song. One problem is maintaining the association between various types of processing on the media signal or its metadata.

The following disclosure describes several methods, devices and applications for processing metadata, including but not limited to, technology to embed metadata in a media signal, and technology to process metadata that will be or has been embedded in the media signal.

The invention provides various methods, systems and devices for associating metadata with media signals, such as image and audio signals. One aspect of the invention is a media signal capture device including a recorder for capturing a media signal, and a steganographic encoder for encoding auxiliary data in the media signal. This device may encode a variety of types of data into media signal at the time of recording. Examples of data types include attributes of the media signal, a reference to external data (e.g., metadata stored in a computer network), authentication data used to authenticate the media signal, etc.

Another aspect of the invention is a media signal capture device including a recorder for capturing a media signal, a processing unit for associating auxiliary data with the media signal, and an interface for receiving session parameters that govern operation of the media signal capture device during a session. The session parameters may be used to control a variety of functions on the device. One use of the session parameters is to specify auxiliary data to be associated with media signals captured by the recorder during a session.

Another aspect of the invention is a method for associating auxiliary data with a media signal. The method extracts a steganographic reference to auxiliary data in the media signal. It then queries a metadata database to request the auxiliary data associated with the media signal using the extracted reference to access the auxiliary data in the metadata database. The method receives the auxiliary data from the database.

Brief Description of the Drawings

Fig. 1 is a block diagram illustrating an example of a digital camera.

Fig. 2 is a block diagram illustrating various connectivity configurations for transferring data to and from an image capture device.

Fig. 3 is a diagram illustrating an application of steganographic links to metadata in images.

Fig. 4 is a diagram illustrating the use of steganographic links to access metadata from different imaging systems.

Detailed Description

Introduction

There are many applications for associating auxiliary data with media signals captured in a media signal capture device such as a camera, scanner, audio recorder, three-dimensional model capture system, etc. A short list of these applications include:

- managing copyrights,
- authenticating the media signal,
- describing objects within an image or other media signal,
- describing the context of the image or other media signal (time, place, subject, camera properties),
- facilitating media object searching based on content,
- uploading and organizing media signal objects from capture devices in library databases,
- sharing media signals over networks, such as the Internet
- linking derivative media signals to originals.

The following sections describe various implementations of image capture devices and related systems that associate various forms of data with images. The sections discuss associating data in images using steganographic and other techniques. Later sections describe how the similar technology may be used to associate data in other media signal types, including but not limited to audio signals.

Steganographic methods can encode data in an image, including identifiers and references that associate the image with additional data stored outside the image itself. In some applications, the capacity of the images to hold a steganographic signal, such as an imperceptible watermark, is sufficient to store the data associated with the image. In other applications, it is useful to store additional data elsewhere, and refer to it through a reference hidden in the image.

One way to associate data with an image is to store the data in the image container (e.g., a file), but outside the image. Yet another way is store the data in a location external to the image file, and create an association between the image file and the external data. In this case, the image may be associated with the external data via a reference encoded in the image itself or in the image file that refers to the external data.

Data associated with a digital object, such as an image, is sometimes referred to as "metadata."

In some applications, the image capture device enables users to specify the types of data as well as specific items of data to be associated with images captured in it. The data "type" describes what a data item represents, while the data "item" refers to the actual data associated with the image. Some examples of data types include the time, place, and subject of the image, and examples of corresponding data items include: 12:30 PM, Times Square, Mom (corresponding to data types of time, place and subject).

The user may specify the data types through the user interface of the image capture device, or through the user interface of an external device or system, which in turn, communicates the desired data types to the image capture device. Camera user interface components, such as buttons or voice recognition modules, enable the user to change settings of the device anywhere, without the need to link it to external device. Data entry and device configuration through external devices, such as a personal computer, personal digital assistant or phone, provides a number of advantages, including remote control of the camera, access to more user friendly user interfaces, and more powerful data manipulation and storage than is capable on the camera.

In addition to specifying the data type, the user may also specify actual data items to be associated with images. Again, the user may specify the data items through the user interface of the image capture device, or through the user interface of an external device. In cases where the user supplies data items to the external device, these items may be downloaded to a storage device on the image capture device, associated with images at the time of or after image capture, and later transferred from the device along with the associated images to external storage. Alternatively, the data items may be kept in storage external to the image capture device and associated with selected images by reference, such as through an identifier that matches an identifier hidden in the image. For example, the camera or some other image management system can insert a stegranographic link (e.g., in an image watermark) that associates the image with the desired data items.

Image Capture Devices and Connectivity to External Devices and Systems

The methods and systems for associating data with images can be implemented in many different types of image capture devices, including conventional film cameras, digital cameras and scanners. To simplify the discussion, the following description uses digital cameras as an example of one type of image capture device.

Digital Cameras

The design of digital cameras is well understood to those skilled in the art, so is not belabored here. Fig. 1 shows an example of a camera 10, including its user interface 12 and its internal architecture.

The camera 10 includes an optical system 14, an image sensor 16, and an image formatter 18. The optical system contains the camera's lens, focus control, and other optics components that control the transfer of light to the camera's sensor 16. The sensor is comprised of an array of discrete sensor elements arranged in clusters sensitive to three primary colors (e.g., red, green, blue). Two common types of sensors are CCD and CMOS sensors. The image formatter includes an analog to digital converter to convert signals from the sensor elements to digital form. It also includes a color space converter to map the signal into a desired color space, such as RGB or YUV. The formatter transforms the image signal into a form suitable for further processing and storage and stores it in the camera's memory subsystem.

Because the specific interconnect varies with the implementation, Fig. 1 depicts a general interconnect 22 that represents the data and control path among various components in the camera. In addition to the image capture components described above, the camera includes a processing unit 22, a memory subsystem 20, and various I/O devices. The camera may include one or more processing devices, such as a microprocessor, and a DSP.

The processing unit executes an operating system, such as VxWorks real time embedded operating system in the Digita Operating Environment from Flashpoint, Inc., or Windows CE from Microsoft Corporation. Application programs supporting functions described throughout this document may be developed using software development environments designed for these and other commercially available operating systems, such as Tornado Tools from Wind River.

A steganographic embedder may be implemented as an application program that executes on the processing unit, or in special purpose hardware that has access to the memory subsystem.

The memory subsystem 20 includes a combination of ROM, RAM, and removable storage devices such as a flash memory card.

The I/O devices include a display 24, and input controls 26. The upper portion of Fig. 1 depicts an example of the rear panel of the camera showing user interface components on the camera. The panel has buttons and switches 30, 32, 34 that control operating modes of the camera and display modes on the display screen 36. It also includes scroll buttons 38-44 that enable the user to scroll through options on various display screens.

The camera is equipped with one or more external interfaces to transfer images, image related data, and operating parameters to and from external devices. The type and number of interfaces for external connectivity vary from camera to camera, and include:

- ports 50 for wire connections to external devices such as serial ports, USB ports, parallel ports, PCI, Firewire or Ilink ports (IEEE 1394 and USB2 ports), and
- transceivers and receivers 52 for wireless connections such as an infrared transceiver, RF transceivers (Bluetooth transmitter/receivers), FM receivers, etc.

The camera may also include a cellular or conventional modem 54 for transferring data to and from a telephone network. In addition to transferring images and data via connections to external devices, the camera can also receive and send data via a removable memory device.

Connectivity to External Devices

The camera's connectivity features enable it to upload images and data to external devices, and enables external devices to download operating parameters and image related data (e.g., image metadata). There are numerous connectivity configurations, including wired and wireless connections to stand-alone and networked devices.

Fig. 2 is diagram illustrating some examples of configurations for connecting the camera with external devices. As shown, the camera 100 may connect directly to a communication network 102, like the Internet, it may connect to a networked device such as a personal computer or telephone (104), and finally, it may connect to a stand-alone device 106.

In order to connect to a network, the camera may have a cellular or conventional modem or a network adapter. It may be connected to a networked or stand-alone device via a communication interface such as the ones mentioned in the previous section.

Fig. 2 highlights some of the connectivity scenarios made possible by these connectivity components in the camera. The connectivity scenarios can be grouped into two principle categories: 1) transferring data and operating parameters to the camera; and 2) uploading images, data associated with the images, and operating parameters from the camera.

Transfers to the Camera

One configuration is to transfer the desired information through a direct connection to the camera, such as through the camera's serial port, USB port, parallel port, Firewire or Ilink port, infrared transceiver port, or RF transceivers port. In this scenario, the source of the information may be a networked or stand-alone device.

Another configuration is through an indirect connection from the source of the information to the camera. The indirect connection may include one or more hops through a wired or wireless connection. An example of a wired connection is where the camera 100 is connected to a network 102, such as the Internet, and another device, such as a server 108, sends the information through the network to the camera, which is connected to the network. A useful application of this configuration is where a user of a client computer 110 designates operating parameters and metadata through an interactive web site. The web server 108, in turn, transfers the operating parameters and metadata to the camera through the network 102.

Another related configuration is where a user specifies desired parameters to a server computer 112, which in turn, sends the data to the camera through a wireless connection or broadcast. One example of a wireless connection is through wireless

network to a cellular modem in the camera. Example of a wireless broadcast include transmitting the data from the server to a FM transmitter (e.g., the radio tower 114) or satellite transmitter (116, 118) to a compatible receiver in the camera.

Uploading Data from the Camera

Many of the same configurations outlined above for transferring data to the camera apply to uploading data from the camera as well. However, as practical matter, cameras have more limited resources to process and transmit data. One way to address these limitations is to incorporate into the camera a high bandwidth interface to transfer large amounts of data, such as the images and their related metadata, as well as a low bandwidth interface for transferring smaller packages of data, such as an identifier or set of control signals. The high bandwidth interface may be implemented using a port that can communicate large amounts of data efficiently, without unduly complicating the circuitry on the camera. Examples of such ports include a USB, firewire or Ilink port (IEEE 1394 and USB2). The low bandwidth interface may be used to implement a wireless signal transmitter, such as cellular modem transceiver, or other wireless signal transmitter, such as FM, RF, infrared, etc.

Image Data Configuration

As noted above, there are two principle categories of methods for configuring the camera to specify its operating parameters, and to specify the types of auxiliary data to be associated with images: 1) through the user interface of the camera; and 2) through an external device. The following sections provide examples of devices for configuring the camera and methods of operating these devices.

Camera UI

The camera UI may be implemented with many different combinations of input and output devices. The input devices may be implemented using combinations of hardware controls, such as buttons, switches, dials, cursor control devices, etc., and soft controls, such as touch screens, soft buttons, scroll bars, and check boxes displayed on a display device. The camera may also be configured to receive voice input through a microphone, voice codec, and voice recognition hardware and software.

Similarly, the output devices may produce visual and/or audio output. For example, the camera may have a display screen, with or without support for video output. In addition, it may have audio output, and allow for playback of voice instructions, and output of a text to speech synthesis system.

In the example depicted in Fig. 1, the user manipulates the user interface (Fig. 1) to specify the data that is to be associated with a picture or series of pictures. The user may specify the data type to be associated with a picture, and then allow the camera to supply the actual data from its storage or from an internal device (e.g., clock for the time, GPS for the location, etc.). The data in the storage device may, for example, be downloaded to the camera from an external source. Additionally, the user may specify the actual data to be associated with each picture, either in advance, or as he snaps the pictures. For example, the photographer might enter his name, and the names of the people or things in the picture. The photographer may opt to enter the data once, and then have it linked to several pictures in a virtual roll. A virtual roll is a set of images that constitutes a "roll."

In one particular implementation depicted in Fig. 1, the user interface accepts user input via the buttons 30-34. Using known UI techniques, the user can use the scroll buttons 38-44) to scroll through a list of selections displayed on display screen 36 until a desired selection is presented. Once the list has been scrolled to the desired entry, the user can actuate a second button (e.g., 32-34) to effect that selection. The data types associated with an image or set of images can be of various classes. One class can identify the photographer, another class can identify the subject, etc.

For the class of photographers, the scrollable list of selections can include a default list of descriptors (e.g., Mom, Dad, Child1, Child2, #1, #2, etc.), supplemented (or replaced if desired) by a list that is customized by the owner of the camera (e.g., Bill, Kristen, Hannah, David, etc.).

The class of subjects can similarly include a default list (e.g., Birthday, Vacation, Anniversary, Wedding, House, Car, Pet, etc.) and/or a customized list (Uncle Harry, Yellowstone, Mushrooms, Seascapes, etc.) The user interface for selection of subjects may permit selection of several subjects – providing alternate descriptors for an image.

A descriptor selected by the user can be used to encode the picture just-snapped, or can be used to encode pictures thereafter-snapped. A descriptor embedded in the image may be in the form of text, or a number that refers to metadata stored outside the image.

Rather than having a cumbersome interface built into the camera, the camera may support one or more plug-in user interface peripherals, such as a keyboard. Alternatively, the configuration data in the camera may be synchronized with configuration data in an external device via a wire or wireless connection.

In some applications, the photographer may be intentionally precluded from controlling the data associated with pictures. This feature is important in applications where there is concern that the photographer might tamper with the metadata associated with an image. For example, the photographer might try to alter the time, place or subject to create a false or misleading photographic record. To prevent such tampering, the photographer's employer or supervisor can set the operating parameters and make data type selections from an external source. Operating parameters may be used to set certain types of data, such as the time, or to disable the photographer's ability to change certain parameters.

In order to implement such features, the camera supports a variety of different operating modes. In a session mode, the camera operates under the control of parameters that govern that session. The operating parameters for the session may be established through the user interface of the camera, or from an external device. In addition, the user may initiate a session, or an external device may initiate the session.

When the camera receives the operating parameters for the session, it makes all settings to comply with the instructions specified in the operating parameters. For example, if the session parameters instruct the camera to set the time, date, place or subject for the session, the camera does so. The session parameters may also specify that the user is to be precluded from altering the operating parameters for the duration of the session. For example, the user may be precluded from altering data items or data types associated with images snapped during the session or from altering certain camera functions, such as a time keeping function, a GPS function, etc. during the session.

The duration of the session may be set and measured using certain operating parameters. For example, the session may be in effect for specified period of time, for selected number of images, for selected GPS locations within a defined range, etc. In addition, the session duration may be specified in terms of certain events, such as a configuration event in which the session is configured, and an upload event, where the images snapped during a session are uploaded from the camera. Using this approach, the one configuring the camera can specify that the session shall extend from the configuration event to some other event, such as the act of uploading the images in the session.

The camera can be programmed to operate according to the parameters that govern the session. It may disallow the user from capturing images when the camera travels outside a particular location specified in the session parameters and monitored by the GPS unit within the device. Similarly, it may disallow the user from capturing images outside a predetermined time interval specified in the session parameters. To this end, the camera has a time clock that keeps time and is synchronized to a master clock to avoid errors that might occur due to user tampering or traveling through different time zones. The time clock can be set permanently to run synchronized with a master clock or can be periodically synchronized by an external master clock via a wire or wireless connection. Just as the parameters can prevent certain actions outside a given time span or geographic area, they can also selectively allow certain actions within a given time span or area. In addition, the time clock and GPS unit can be used to insert or link a time and place stamp to every image that is captured during a session or otherwise.

The session parameters can govern when and where the images are steganographically marked and uploaded. For example, the parameters may specify that the images are to be steganographically marked at the time of image capture, or at some later time. Similarly, the parameters may specify that the images are to be steganographically marked at the location of image capture or some other location (within some geographic region), as determined by the GPS unit within the device. Similar parameters may be established to specify a time or time range for when the image or images may be uploaded to an external storage device or processor.

A session may be tracked and associated with session related metadata by a session identifier encoded in the image, the image file, or its metadata. For example, the session identifier may be a number or message embedded steganographically in the image or metadata associated with the image.

Configuration via External Devices

As noted in previous sections, the data to be associated with images may be provided by an external device. The external device may set operating parameters that control the operation of the camera, including how and what data it associates with images. The external device may also set the data types as well as the actual data to be associated with images in the camera.

In some applications, a computer can be programmed to perform this function automatically for one or more cameras. For example, a server may be programmed to broadcast operating parameters and data to several cameras in the field.

In other applications, a user may enter the desired operating parameters and data to be associated with the images in the camera. In client-server scenario, for example, a user of a client device may submit desired operating parameters and data to server, which in turn, sends the information to the camera. In an alternative scenario, the user can enter this information via an application program executing on his PC, or PDA, and then instruct the application to download the information to the camera via a direct wire or wireless connection to the camera.

Image Data Sources

The data associated with images in the camera may come from a variety of sources. One source of data is the camera UI. Another source is the internal components and peripherals of the camera, such as a time clock, GPS device, camera components, camera software, etc. Yet another source is an external device. In this case, the camera will either have the data in its memory, after receiving it from the external source, or the camera will have a reference to data, which is stored on external device. As detailed further below, the reference may be an pointer, address or some other form of identifier that is encoded in the image.

Storage of Data Types and Data Items Associated with Images

A related design issue is where to store the data associated with an image at various stages of image processing. These stages include: 1) before configuring the camera; 2) after configuring, but before snapping the picture; 3) after snapping, but before transferring the associated image from the camera; and 4) after transferring the image from the camera.

Before Configuring the Camera

Before configuring the camera, the data types and data items to be associated with images may be stored in the camera or in one or more external storage devices, depending on the application.

The camera may maintain data types and items within the memory subsystem built into the camera (e.g., ROM or RAM) or within removable memory devices, such as a floppy disk, flash memory card etc. In some implementations, the camera maintains a set of data types that a user, application program or device may select to associate with images. A user can select from among these desired data types from the user interface of the camera or from an external device.

In applications for external configuration, a user, device or application program may maintain this data in memory of a computer, such as personal computer, personal digital assistant, server on the Internet, etc.

After Configuring the Camera

After configuring the camera, selected data types and items to be associated with images may be stored in camera memory, or in external storage. In either case, the camera maintains an association between the images to be captured and the data to be associated with those images. In cases where the image metadata is stored externally, the camera maintains a reference to the external data, such as an identifier number, pointer, or address.

After Capturing A Target Image

After capturing a target image in the camera, the camera may store data items associated with the image in the image itself through steganographic encoding, in the

image file, outside the image file but within camera memory, and in external storage. The "target" image refers to the image that is associated with selected data types and data items. In the last two cases, the camera maintains a reference between the target image and the associated data. The reference may be encoded in the image steganographically or in the image file.

After Transferring the Image from the Camera

After transferring the image from the camera, the options for storing the data associated with the target image remain the same, yet the camera or some external device or process may transfer the data from one location to another. For example, an external steganographic encoder can embed some of the data in the image. In addition, an external process or device can transfer data to or from the image metadata in the image file. Image data stored externally may be transferred from one database, e.g., a configuration database, to another database, e.g., an image library or metadata database. For example, upon uploading an image to an image database, the uploading process can signal the configuration database to transfer image related data to the image or metadata database.

Associating Image Data with Images

The previous sections highlighted several methods for associating data with images. These methods include: steganographic encoding data in the image, storing the data within the image file (outside the image), storing the data outside the file and associating this external data with a reference stored in the file or encoded in the image. The following sections describe examples of these methods in more detail.

Embedding Auxiliary Data within an Image Using Steganographic Methods

The art of hiding auxiliary data into still and moving images is relatively advanced. Most techniques make slight changes to the image - e.g., by changing data representing the image, whether in the form of DCT coefficients, wavelet coefficients, pixel values, or other interchangeable representation - to thereby encode the auxiliary information. The changes are so slight as to be essentially imperceptible to the human visual system. Exemplary watermarking techniques are shown in 5,841,886 to Rhoads and U.S. Patent 5,915,027 to Cox.

For additional information about a digital watermarking form of steganographic embedding and reading, see co-pending US Patent Application No. 09/503,881 filed February 14, 2000, which is hereby incorporated by reference. The above references describe how to embed auxiliary information steganographically in various media objects, including still image, video and audio signals.

The steganographic encoder may be located within the camera or in external process or device. In either case, the encoder can be implemented in software, hardware or a combination of both.

An encoder implementation in the camera operates on images stored in the camera's memory system. For each image, the encoder converts auxiliary data to be embedded in the image into watermark signal and combines the watermark signal with the image. This auxiliary data may include one or more references, a machine instruction or set of instructions, and other data items about the image. A reference is a data item, such as identifier number, address or pointer. It may be used to identify the image and reference additional data related to it.

The camera-based encoder obtains auxiliary data to be embedded in an image from memory, or some other device in the camera. Recall that during configuration of the metadata, the user or some external device or process specifies the data types and data items to be associated with images. At encoding time, the encoder retrieves data designated for embedding in the image, converts it into a watermark signal and combines it with the associated image. To reduce the amount of data embedded in the image, the encoder may embed one or more references that identify data associated with the image that is stored outside the image.

There are many places to implement the encoder outside the camera. In one implementation, the encoder is implemented as part of a process for uploading the image from the camera. In this implementation, the data for embedding in the image may come from the camera, an external device, or a combination of both. During the configuration stage, a configuration process specifies that data to be associated with image, including any data to be embedded in the image. As explained above, this data may be stored on the camera or an external device. The uploading process transfers the images from the camera, along with any data associated with the images.

As part of the uploading process, an encoder then encodes auxiliary data designated for embedding in the image into the image. As in the camera-based process, this auxiliary data may include one or more references that associates the image with other auxiliary data stored outside the image. This type of reference avoids the need to transfer metadata into the camera. Rather than transfer such data into the camera, metadata may be configured and maintained on an external device, and referenced to the image via a reference encoded into a watermark in the image. Conversely, the uploading process may move data associated with an image from the camera, store it in a metadata database, and reference the entry in the database via a reference encoded in the watermark.

Embedding Auxiliary Data in the Image File

The camera, or an external process, may also embed auxiliary data in the image file, but outside the image. To support this type of association, the image is stored in a file format that allows metadata to be stored in the file along with metadata. For example, the format may specify that the data is to be stored in the file header. This approach of associating data with an image has advantages, but is more susceptible to intentional or unintentional manipulation.

In this case, a reference embedded in the image can be used to correlate the image with the correct metadata. This is particularly useful in applications where the metadata is placed in the image file by a process external to the camera. In these cases, it is possible that the metadata may be improperly assigned to a particular image. In addition, various image processing applications may remove or alter the image metadata stored in the image file. The data steganographically embedded in the image can be used to authenticate the metadata stored in the image file. One form of authentication is to match a reference number embedded in the image with a reference number in the image file metadata. More sophisticated forms of authentication may be implemented as well.

For example, both the number in the file metadata and the watermark may be encrypted. Also, the number may be a digital signature derived from the image, such as by performing a hash function on the image sample values. The digital signature has

the added advantage that it can be used to determine whether the image has been modified. For additional security, the digital signature can be encrypted, and then embedded in the watermark and placed in the image file metadata.

Maintaining Auxiliary Data Separate from the Associated Image

As noted above, the auxiliary data associated with the image can be maintained separately from the image. A reference to this external, auxiliary data may be embedded in the image (e.g., in a watermark), in the image file metadata, or both.

Data Types

The types of data that can be associated with an image are numerous and vary with the application. The image data framework described above supports a variety of different data types, including:

- who took the picture (the photographer,
- who or what is the subject of the picture,
- where was the picture taken (e.g., entered by user, or provided by GPS device),
- when was the picture taken (e.g., date and time of day),
- how was the picture taken, including camera specifications such as brand, model, manufacturer, and type of color converter, lens, sensor, flash, etc.
- picture specific device data, including shutter speed, flash used, camera settings, focus, distance of subject from camera, resolution of image, light levels,
- why was the picture taken? entertainment, legal record, medical record, real estate, business transaction record, etc.
- image type,
- copyright conditions,
- copyright owner and owner of copy,
- view data- the camera location and subject location,
- comment- e.g., user comment
- picture identifiers, e.g., industry or application specific identifiers,

- collection data, including collection ID, collection caption, collection members,
- Image quality parameters,
- Color profile,
- Image integrity- Digital signature, encryption key (e.g., public encryption key),
- Sound annotation, or reference to sound annotation,
- Language specifier, for elements of the metadata,
- view region- Advanced Photo System Print Aspect Ratio (PAR) selections of conventional, HDTV, and panoramic,
- user address, e.g., email or physical address,
- reference to derivative work- parent image and its derivatives,
- reference to alternative images- e.g., alternative view, color space, resolution, etc.
- region specification- describe a region in a picture, e.g., the pixels that represent an object in the picture,
- compression format of image, compression format of image data (e.g., compression format of image metadata),
- encryption type of the image, and the image data (encryption of image metadata),
- references to other information (e.g., pointers, network links or addresses, phone numbers, etc.)
- machine instructions or sets of instruction, e.g., instructions that control rendering of the image, that disable or enable certain types of editing operations, that control compression, decompression operations, etc.

Metadata Applications that Exploit Steganographic Data

Steganographic encoding of data enhances existing applications of image metadata and enables a variety of novel applications. The following sections describe some of these applications.

Persistent Steganographic Data and Metadata Servers

Steganographic encoding of auxiliary data in an image enables persistent linking of the image to its metadata. Metadata that is stored within an image file, yet outside the image, is vulnerable to intentional and unintentional manipulation. Whenever an application or device processes the image, it may remove or alter the associated metadata. One solution is to store the metadata separately from the image. However, this approach requires that there be a reliable way to link the metadata to the image as it passes from one image processing application or device to the next. Steganographic encoding provides such a link between the image and its metadata. This link is referred to as a persistent staganographic link because it remains part of the image data through various image processing operations, including transfer to and from the analog domain (e.g., printing to image capture).

Fig. 3 is a diagram illustrating a metadata server application that uses a persistent steganographic link to ensure that various devices and applications that process an image have access to its metadata. This diagram refers to "compliant" and "non-compliant" metadata applications. A compliant application refers to a device or software process that adheres to standard guidelines for maintaining image file metadata. A non-compliant application is a device or process that does not adhere to such guidelines, and may alter the metadata in unintended ways.

Starting from the upper left of Fig. 3, a compliant application adds metadata to the image, and sends the metadata to a metadata server. The server stores the metadata along with a reference (e.g., unique number) to the image. This reference serves as a link to the image, and matches the reference steganographically embedded in the application. This example scenario assumes that the form of steganographic coding is a digital watermark. Either the compliant application, or some other previous process embeds the watermark, including the reference, in the image.

The compliant application produces an image file that includes the digital watermarked image (DWM) and the metadata. One example of such an application is the application for uploading images from cameras or from PCs to a server on the Internet. This application embeds the watermark in the image and forwards the

metadata to the metadata server. Note that the server application for uploading images and the metadata server database application may be implemented in the same server or a group of servers.

Next, a non-compliant application gets this file, and removes or corrupts the metadata, leaving only the watermarked image.

Noticing that the image does not have metadata, the next compliant application sends a request to the metadata server for the image's metadata. The compliant application, equipped with a watermark detector, screens the image and extracts the reference to the image's metadata. It then forwards this reference to the metadata server, which returns the metadata. The format of the metadata may be based on XML or some other standard or custom data format. Preferably, the metadata format is sufficiently general to be compatible with many different devices and applications, but this not a requirement. The compliant application produces a new image file, including the watermarked image and its restored metadata.

Metadata Router

This concept can be extended beyond a single system by adding another component, the metadata router. Assume a collection of different systems, each with its own metadata server, and each tracking its own images. Fig. 4 depicts an example of three different systems, each having its own metadata server. Each of the metadata servers handles requests from imaging applications within its system. If an image from one system is acquired by another system, the new system will not have any associated metadata. Therefore, any application in the new system that tries to retrieve metadata from its metadata server will fail; it will find no information. If however, the new metadata server can determine which metadata server does have the information, it can request the image metadata from the other metadata server.

The metadata router is the component that can help resolve which metadata server contains information about a particular image. The metadata router can operate either on a watermarked image, or a reference extracted from an image. In the former case, the requesting system has been unable to detect the metadata reference (e.g., it cannot detect a watermark), and thus, has forwarded the image to the router. The router then performs one or more watermark detection operations to extract the reference, and

if successful, maps the extracted reference to the metadata server by using the extracted reference as a key to the metadata server in its database.

In the latter case, the requesting system has extracted the metadata reference, but does not maintain the metadata for that reference. The metadata router maps the reference to the appropriate metadata server by using the reference as a key to the metadata server in its database. It then redirects the request to the metadata server, which returns the requested metadata. The server having the metadata may return the metadata to the metadata server of the system from which the request originated and/or to the requesting application. This system may be implemented on a computer network, such as the Internet, using conventional networking protocols to communicate requests and return data over the network.

The application may also make the request for metadata by requesting the metadata from the metadata router. The router, using the identifying information extracted from the watermark, redirects the request to the appropriate metadata server. The server maps the reference to the image's metadata and returns the requested metadata to the metadata server of the system from which the request originated and/or to the requesting application.

Searching Metadata

The techniques described above provide powerful applications for searching metadata that extend across different imaging applications and systems. For example, a user of an imaging application in one system can send a search request to the metadata server for that system. The search request can direct a search in one more fields of the metadata (e.g., time, place, subject, etc.) in the metadata database. Using the metadata router, the metadata server can extend the search across systems by forwarding the search request to a metadata router, which in turn, forwards the requests to other metadata servers.

In addition, applications can support image based searching. For example, an end user might find an image of interest. The user then issues a request such as: "find other images like this one" (e.g., taken at a similar time, in a similar place, or having a similar subject). The client application or the metadata server extracts the reference from the image watermark. The metadata server then searches its database for images

that are similar based on the criteria provided by the user, or based on metadata associated with the image. The metadata server can extend the search to other metadata servers by forwarding the request to other metadata servers via the metadata router. If the user finds an image that is not compatible with the system he is using, the same approach outlined above for finding the image's metadata can be used to find the corresponding metadata server and initiate a database search for related images.

Access to just metadata (independent of the picture)

The schemes outlined above facilitate access to metadata independent of the picture. By storing the metadata in a metadata database, applications can access, search and transfer the metadata without the images. This is particularly beneficial where bandwidth and storage is limited because the most common form of metadata, text, is usually smaller in size than the associated image. It requires less bandwidth and memory to transmit and store this text separately from its associated image.

Metadata of an image may also be voluminous in some cases. For example, the metadata may include a sound or video annotation. It is advantageous to be able to store, access and search this type of metadata separately.

Metadata editing (create, read, update, and delete)

The metadata server scheme outlined above support editing of the metadata associated with an image. To edit an image's metadata, a user may access the metadata by extracting the persistent link to the metadata server and issuing a request to the metadata server. The metadata server implements a scheme for managing the rights to edit (e.g., create, read, update, and delete) the image's metadata. For example, the server may require the user to enter authentication information, such as user name and password. In response, the server determines the editing rights by looking them up in its database. Based on these rights, the user may be granted the authority to create, read, update, or delete the metadata.

Metadata Persistence

Persistent steganographic links to metadata ensure the persistence of an image's metadata through various operations, including file conversion (e.g., changing the file

format of the image), file transmission (e.g., sending an image by email, or by wireless transmission), image compression, and image editing. The steganographic data is designed to stay in tact through various forms of image processing.

The persistence of the steganographic link also ensures metadata persistence of various types of data associated with the image, including copyright information. In addition, it supports adding multiple instances of copyright information, for works with multiple owners, and authors. The scheme for managing editing rights described above enables authors who create new works based on existing works to add copyright information to the image. The metadata server may be programmed to notify the copyright owner whenever another author wishes to modify an image. The right to modify a particular image may be pre-specified (e.g., a specified list of authors who have editing rights), or may be requested on a case by case basis. The metadata server may notify the copyright owner by email, for example, asking for authorization to grant editing rights to a particular author. If granted, the metadata server informs the new author of the terms. Then, if the new author excepts the terms by sending a return email or manifesting intent via an interactive web page, for example, the metadata server allows the new author to create a derivative work of the image.

The derivative work inherits the metadata of the original work, including copyright information of the copyright owner in the original work. To associate the metadata for the new image, the metadata server provides a new reference to the new author's imaging application, which in turn, steganographically encodes the new reference in the derivative work. Additionally, the metadata server adds an entry in its database that associates the reference embedded in the new work with its corresponding metadata. This entry may also include a pointer to the database entry for the original work. This scheme for cross referencing earlier works enables the metadata server as well as system users and applications to track the history of an image through various types of editing.

Steganographic linking of images to metadata allows the persistence of an image's metadata to be specified externally by a user, device or application. As noted above, the persistence of metadata is often vulnerable to intentional and unintentional

manipulation. It is difficult for a user to specify which items of metadata are to persist with the image, and under which circumstances.

The metadata server allows users, devices and application processes to specify which items of metadata are to remain persistent, through various forms of processing. The metadata servers and routers, having the appropriate authority, may annotate an image's entry or entries in a metadata database to specify which data items will survive specified types of image processing, or image transfers. For example, if one system requests a metadata server to supply metadata to another system via the metadata router, the metadata server will only supply metadata that is designated to be persistent for the specified type of operation on the image.

The steganographic link to metadata also supports the combination of metadata when two or more images are combined. As noted above, the metadata server may issue a new reference to be steganographically encoded in the new, combined image. The server may combine the metadata by combining the metadata for each component image into one metadata database entry, by inserting reference links in the database entry for the new image to the metadata entries for the component images, or some combination of these approaches.

Metadata Format and Processing

The metadata may be specified using the standard Extensible Markup Language, XML, or some other standard or custom format. The XML standard describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. XML is an application profile or restricted form of SGML, the Standard Generalized Markup Language [ISO 8879]. By construction, XML documents are conforming SGML documents. XML documents are made up of storage units called entities, which contain either parsed or unparsed data. Parsed data is made up of characters, some of which form character data, and some of which form markup. Markup encodes a description of the document's storage layout and logical structure. XML provides a mechanism to impose constraints on the storage layout and logical structure.

A software module called an XML processor is used to read XML documents and provide access to their content and structure. In the implementations based on

XML, the XML processor processes raw XML data on behalf of other application programs, such as an image processing application or a metadata server application. For more information on XML and XML processors, see the XML Standard document, Version 1.0, by the World Wide Web Consortium.

Metadata Security and Authentication

The metadata associated with an image may be secured and authenticated at various stages of processing. These processing stages include: at or shortly after image capture in the camera, upon uploading the image from the camera, within the metadata server, and during transfers of the metadata from one device, application or system to another. One way to secure the metadata is to encrypt it. Another way is to restrict access to it via the metadata server such that only authenticated users, applications, and devices have access to it. Yet another way is to create a digital signature of the metadata, such as by performing a secret hash function on the data to derive a unique signature. This signature can be recomputed for suspect metadata and compared with a signature stored in the metadata database or elsewhere to determine whether the metadata has been modified.

Other Applications

With the growth in popularity of digital image capture devices, there is a growing demand for photo processing and storage services for digital images. Several companies now offer photo-processing services accessible via the Internet. These services create prints of digital photos sent via the Internet and mail the prints to the customer. A related service is providing an on-line database of images. Such services enable customers to maintain a collection of photos in an accessible database, e.g., an on-line database on the Internet.

The metadata database applications described above provide an effective way to manage data associated with images. These applications are particularly applicable to the Internet, where the database information may be made available to a variety of users, imaging devices, application processes and systems.

The image metadata may be maintained in a separate database or in a database integrated with an image database that stores the images themselves. The image

database may contain a private collection of photos or collections of photos from unrelated users.

A related application to maintaining image and metadata databases is tracking transactions involving the images or their metadata. The image or metadata database may keep a history or log file of the transactions associated with an image. For example, as users request processing services on photos, such as creating prints, putting the prints on objects (e.g., shirts, cups, calendars, posters etc.), etc., a tracking application keeps a record of the transaction, listing attributes of the transaction like the date, vendor, service provided, and images subject to the service. The transaction history may then be linked with other metadata and the image itself by a reference, such as the steganographic link embedded in the image. There are a variety of other ways to link the transaction history with an image. For example, the transaction history may be stored in an entry in the metadata or image database associated with the image.

These applications may also be implemented for other media signals, such as audio, video, graphical models, etc. as explained below.

Other Media Signal Types

The technology described above relating to persistent links in images also applies to other media signals, including audio, and video signals, and computer graphics models (e.g., two-dimensional, three-dimensional graphical models and animation). Video is just another form of an image signal, so the same technology applies to embedding, reading and using links and metadata steganographically encoded into video signals. Steganographic processes may also be applied to audio signals as described in the patent documents incorporated by reference in this document. As such, the same applications may be implemented for audio by embedding metadata and/or a persistent link to metadata in an audio signal.

Much of the technology discussed above directly pertains to still image capture devices as well as video capture devices, so no further elaboration is required. Generally speaking, metadata or a persistent link to metadata may be steganographically encoded into a video signal at the time of capture or at some later time and location. A video capture device may be adapted to insert a steganographic

link in one or more video frames as the video signal is being captured, or shortly thereafter, before the encoded signal is transferred from the device. Also, the steganographic link may be inserted in the video signal as it is being transferred to an external device, such as a computer either directly linked or indirectly linked through a communication network (e.g., the Internet).

Similarly, metadata or a persistent link to metadata may be steganographically encoded into an audio signal at the time of capture or at some later time and location. An audio capture device (e.g., an analog or digital audio recording device) may be adapted to insert a steganographic link in one or more audio segments as the audio signal is being captured, or shortly thereafter, before the encoded signal is transferred from the device. Also, the steganographic link may be inserted in the audio signal as it is being transferred to an external device, such as a computer either directly linked or indirectly linked through a communication network (e.g., the Internet).

Once inserted in the media signal, a decoder can then extract the metadata or persistent link to metadata from the media signal. Once a steganographic decoder extracts the link to metadata or metadata itself, the same applications described above for retrieving, processing and using metadata apply. For example, the metadata server and router systems may be adapted to store and control access to metadata for media signals other than images. The same metadata applications that exploit steganographic data for images apply to other media signals as well.

More On Metadata

As noted above, metadata may be steganographically encoded in media signals such as image, audio and video signals. In particular, metadata may be encoded into a digital watermark embedded in a host media signal.

One form of metadata that may be encoded in such a watermark is a metadata digest. One type of a metadata digest provides a synopsis of the metadata associated with a media object. For example, it may include descriptors of the names or types of metadata associated with the media signal. These descriptors can be in the form of alphanumeric or numeric identifiers. The digest may also include an abbreviated version of each type or selected types. Software programs or devices can extract this digest with a watermark decoder to determine the types of metadata associated with a

media signal. Based on the information in the digest, the extracting process can decide how to act on the metadata. One action is to display the digest to the user, and enable the user to decide whether to access the complete metadata via a link to the metadata (e.g., a URL, or dynamic index to a database entry in a local or remote, networked computer system). Another action is to control the processing of the media signal, such as rendering, compression, encryption, editing, etc.

Another form of a metadata digest for encoding in a watermark is a hash of the metadata associated with the watermarked media signal. A variety of known hashing techniques may be used to convert a binary form of the metadata to a hashed metadata digest. A watermark encoder then encodes this hashed metadata into a watermark and embeds the watermark in a host media signal. At decoding time, the hashed metadata may be used to access a complete version of the metadata. For example, the hashed metadata may be used as a database key to look up the associated metadata in a metadata database.

Additionally, the hashed metadata from the watermark may be used to authenticate a copy of the metadata stored outside the media signal. The hashing function used to create the watermark message is applied to the metadata stored outside the media signal. The resulting hashed metadata is then compared with the metadata decoded from the watermark in the media signal to check authenticity of the metadata. As noted above, the metadata may be stored outside the media signal, such as in a file header of a file containing the media signal, a metadata database, etc. For many applications, there is a need to establish the metadata stored externally is the same as the metadata that was originally associated with the media signal and recorded in the watermark embedded in the media signal. The metadata digest provides a mechanism for authenticating the metadata for these applications.

As noted above, time stamps and location stamps are additional forms of metadata that may be encoded into a watermark signal and embedded into an associated media signal. The time stamp can be used to mark several types of events, including, but not limited to:

the time of media signal creation or editing,

the time of watermark encoding into the media signal,

the time of metadata association with the media signal,

the time of transfer of the media signal or metadata from one device to another, etc.

The source of the time stamp varies with these types of time stamp uses. The time may be supplied by the media signal capture device, such as camera or audio recording device. Alternatively, it may be supplied by a media signal editing program or device, a media signal transmission program or device, a metadata creation or editing program or device, a watermark encoder program or device. In sum, the device or program operating on the media signal or metadata may supply the time stamp to mark the time that the device or program processed the media signal, its metadata, or the watermark in the media signal.

The location stamp may be used in the same contexts and applications as the time stamp. A global positioning device or other provider of location may supply the location data included in the stamp. Also, the time and/or location stamp may be included in the metadata digest, either in hashed or unhashed form.

Another way to authenticate metadata is to use corresponding sets of time or location stamps in the metadata and the watermark within the media signal with which the metadata is associated. In particular, the time stamp clock may provide a time stamp for the watermark message, which may include metadata or a metadata digest, and then provide a corresponding time stamp for metadata stored externally. The time stamp in the watermark may then be compared with the time stamp in the external metadata to determine whether the time matches. Similarly, changes to the media signal or metadata may be time stamped in the watermark and in the external metadata. This provides a mechanism to synchronize changes to the metadata or media signal with each other.

As noted previously, additional processing may be applied to the metadata before encoding it into a watermark and embedding the watermark in a host media signal. One form of processing is data compression. The metadata may be compressed and inserted into a watermark in the media signal. Data compression effectively increases the data capacity of the watermark. In addition, the metadata may be encrypted and inserted into a watermark in the media signal. Encryption reduces or

even eliminates tampering with the metadata. In addition, it can be used in conjunction with digital signature technology to authenticate the metadata and its source.

Similarly, metadata stored externally to the media signal may be compressed and/or encrypted as well.

The specific types of compression applied to the metadata are preferably, but not necessarily, data specific to the type of the metadata. Some applications may require metadata to include text, sound, images, video, graphics, and various combinations of these types of data. Text compression codecs may be used to compress and decompress text. Voice data compression codecs may be used to efficiently compress and decompress voice data. Image and video compression codecs may be used to efficiently encode and decode images and video. Audio compression designed for compressing music may be used to compress music files. For metadata in the form of imagery such as still images or video, examples of compression codecs include JPEG, JPEG 2000, MPEG, and H263. For metadata in the form of audio such as music, examples of compression codecs include MPEG (ISO/IEC 14496-3:1999 (MPEG-4 AAC); ISO/IEC 11172-3:1993 Layer III (MPEG-1 Audio Layer 3 "MP3")), ISO/IEC 13818-7:1997 ("AAC"), Q-Design, Windows Media Audio, Twin-VQ, ATRAC-3, Dolby Digital AC-3 ATSC A_52, and ePAC.

Other types of lossy or lossless data compression may be used. Some examples of entropy coding include arithmetic and Huffman coding. Run length encoding and LZ compression may also be used to compress metadata.

Through the use of compression, more types of metadata can be embedded in a watermark within a media signal. For example, an image can carry its own sound data. Consider the case where an image is embedded with a watermark and printed. As part of the embedding process, a sound (such as a voice instruction or comment) can be compressed and embedded into the image's watermark. At decoding time, a camera captures an image, and a watermark decoder extracts the watermark message from the captured image and invokes a decompression program or device to decode and play the sound. In effect, the printed object talks to the user by virtue of the voice data encoded into the printed image.

Additional metadata may be stored in video because each frame provides another opportunity to convey a different message in a watermark for that frame. Similarly, voice or other data may be compressed and encoded within audio frames (discrete segments of an audio sequence) of a music file. This voice data can be decoded and played to announce the title of the song or provide other information associated with it.

Encryption may be used to encrypt metadata encoded in a watermark and stored externally to the media signal. Some examples of public key cryptography include RSA, DES, IDEA (International Data Encryption Algorithm), skipjack, discrete log systems (e.g., El Gamal Cipher), elliptic curve systems, cellular automata, etc. Public key cryptography systems employ a private and public key. The private key is kept secret, and the public key is distributed to users.

One use of encryption is prevent tampering with metadata. Without an encryption key, a user or device cannot access metadata that has been encrypted. Metadata embedded in a media signal via a watermark and stored externally can be encrypted. Later, to check authenticity of the metadata, a device or application with the key decrypts the metadata from the watermark and from an external source. Then the decrypted metadata from both sources is compared to check for differences in the metadata that evince tampering. It also possible to perform metadata authentication by encrypting one or the other of the metadata in the watermark or metadata stored externally to the media signal. The decrypted metadata may be compared with the metadata that has not been encrypted to check for differences that evince tampering.

Encryption techniques may be used to create a digital signature that identifies the source of the metadata or media signal. To digitally sign metadata or media signal, the originator of the metadata encrypts the metadata with a private key. The private key is uniquely associated with the originator. Those users, devices or programs having a corresponding public key verify that the metadata has originated from the holder of the private key by using the public key to decrypt the metadata. If the metadata can be decrypted with the public key, then some indicator can be displayed or output indicating that the metadata is valid (i.e. has been encrypted with the private key). This form of authenticating metadata with a digital signature applies to metadata

within a watermark in a media signal or stored externally to the media signal. Authentication of a digital signature can be integrated with the process of decoding a watermark message.

Encryption is a particularly useful way of ensuring that sensitive metadata is not tampered with. Some examples of sensitive metadata include time stamps, location stamps, metadata digests, content signatures or metadata signatures. For some applications, there is a compelling need for the user of a media signal to be able to prove that the metadata is accurate. By encrypting the metadata, or at least the sensitive portion, it significantly reduces the chances that encrypted metadata will be tampered with. If the encrypted metadata is tampered with, it is more likely that the tampering will be apparent when it is attempted to be decrypted or when it is compared with another copy of the metadata.

A content signature is type of metadata used to define some distinguishable and identifying attributes of a media signal. For example, it may be a hash of a media signal, such as a representation of salient features of an image (eyes and nose locations of a person's photo) or sound file (a statistical features like average energy, autocorrelation with set delay, power, frequency coefficients, or other salient features like locations of high to low energy transitions, etc), a low pass filtering of the image or audio samples, the most significant bits of the image or audio, etc. The content signature may be computed and stored in metadata. Then, to authenticate a media signal, the content signature is recomputed and compared with the content signature in the metadata. Differences between these signatures are output to the user as an indicator of the validity of the metadata or the content.

A metadata signature is a type of metadata used to define some distinguishable and identifying attributes of a media signal's metadata. Similar to the content signature, the metadata signature may be a hash used to authenticate the validity of the metadata. The metadata signature may be computed and stored along with metadata at the time of creation or editing of the metadata or the associated media signal. Like the content signature, it may be encoded in a watermark in the media signal, stored externally to the media signal, or both. To check the validity of the metadata, the hash is recomputed for the metadata in question and compared with the previously computed

metadata signature. Differences may be displayed or otherwise output to the user as evidence of tampering.

The preceding sections describe several methods for encoding metadata into media signals and for authenticating the metadata. Various combinations of these methods may be readily implemented based on the above disclosure. For example, metadata may be compressed, digitally signed, encrypted and encoded into a watermark within the associated media signal. In a decoding process, the metadata may be decoded from the watermark, decrypted, verified by its digital signature, decompressed, etc. Elements of the metadata in the watermark may be used to authenticate the media signal. Also, the metadata may be compared and analyzed with respect to a version of the metadata stored externally the media signal, whether in the file header of the media signal, in a remote metadata database, or elsewhere. Various combinations, sub-combinations and arrangements of these processing stages are possible too. The metadata may include a metadata digest, time stamp, location stamp, content signature, metadata signature, or any combination of these and other metadata types. The detailed description of an implementation for image capture devices applies to other types of devices and programs for creating or editing other media signal types. In place of the image capture device in Figures 1 and 2, for example, one could substitute a device, system or application for capturing, editing or creating other media signals. Each of the operations for associating and processing metadata that apply to images also apply to other media signals.

Concluding Remarks

Having described and illustrated the principles of the technology with reference to specific implementations, it will be recognized that the technology can be implemented in many other, different, forms. To provide a comprehensive disclosure without unduly lengthening the specification, applicants incorporate by reference the patents and patent applications referenced above.

The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings

with other teachings in this and the incorporated-by-reference patents/applications are also contemplated.

WE CLAIM:

1. A media signal capture device including:

a recorder for capturing a media signal; and

a steganographic encoder for encoding auxiliary data in the media signal.

2. The media signal capture device of claim 1 wherein the auxiliary data describes attributes of the media signal.

3. The media signal capture device of claim 1 wherein the auxiliary data includes a reference to auxiliary data stored outside the media signal.

4. The media signal capture device of claim 1 wherein the auxiliary data includes authentication data for authenticating the media signal.

5. The media signal capture device of claim 4 wherein the authentication data is derived from the media signal.

6. The media signal capture device of claim 1 including an interface for receiving the auxiliary data from an external device.

7. The media signal capture device of claim 1 including an interface for receiving an operating parameter specifying a type of auxiliary data to associate with the media signal.

8. The media signal capture device of claim 1 including an interface for receiving session parameters that govern operation of the media signal capture device during a session.

9. The media signal capture device of claim 8 wherein at least one of the session parameters instructs the media signal capture device to preclude a user from altering a device setting during the session.

10. The media signal capture device of claim 8 wherein the session parameters specify auxiliary data to be associated with a media signal captured in the device during a session.

11. The media signal capture device of claim 1 wherein the recorder comprises an image sensor for capturing an image or images, and wherein the media signal comprises an image signal.

12. The media signal capture device of claim 1 wherein the recorder comprises an audio recorder for capturing audio signal, and wherein the media signal comprises an audio signal.

13. A media signal capture device including:

a recorder for capturing a media signal;

a processing unit for associating auxiliary data with the media signal; and

an interface for receiving session parameters that govern operation of the media signal capture device during a session.

14. The media signal capture device of claim 13 wherein the session parameters specify auxiliary data to be associated with media signals captured by the recorder during a session.

15. The media signal capture device of claim 13 wherein at least one of the session parameters instructs the media signal capture device to preclude a user from altering a device setting during the session.

16. The media signal capture device of claim 13 wherein a session identifier is steganographically encoded in the media signal or metadata associated with the media signal in the session.

17. The media signal capture device of claim 13 wherein the recorder comprises an image sensor for capturing an image or images, and wherein the media signal comprises an image signal.

18. The media signal capture device of claim 13 wherein the recorder comprises an audio recorder for capturing audio signal, and wherein the media signal comprises an audio signal.

19. A method for associating auxiliary data with a media signal, the method comprising:

extracting a steganographic reference to auxiliary data in the media signal;

querying a metadata database to request the auxiliary data associated with the media signal using the extracted reference to access the auxiliary data in the metadata database; and

receiving the auxiliary data from the database.

20. The method of claim 19 including:

using the auxiliary data received from the database to create a media signal file including the media signal and the auxiliary data.

21. The method of claim 19 including:

sending authentication data to the metadata database to request access to the auxiliary data associated with the media signal.

22. The method of claim 19 including:

sending a request to the metadata database to edit the auxiliary data associated with the media signal.

23. A computer readable medium having software for performing the method of claim 19.

24. A method for associating auxiliary data with a media signal, the method comprising:

maintaining a database of auxiliary data items associated with media signals, each item being associated with a media signal via a reference steganographically encoded in the media signal;

from a requesting application, receiving a request for auxiliary data associated with a media signal, the request including a reference extracted from the media signal;

using the reference to locate the auxiliary data associated with the media signal in the database; and

returning the auxiliary data corresponding to the reference to the requesting application.

25. The method of claim 24 including:

determining whether the requesting application has access rights to the requested auxiliary data.

26. The method of claim 24 including:

determining whether the requesting application has editing rights for the requested auxiliary data.

27. A computer readable medium having software for performing the method of claim 24.

28. A method for associating auxiliary data with a media signal, the method comprising:

maintaining a database of steganographic links and metadata databases associated with the steganographic links;

from a requesting application, receiving a steganographic link extracted from a media signal, the link referencing auxiliary data about the media signal;

using the steganographic link to locate a metadata database that stores the auxiliary data associated with the media signal; and

forwarding the steganographic link to the metadata database that stores the auxiliary data associated with the media signal.

29. A computer readable medium having software for performing the method of claim 28.

30. In a method of associating auxiliary data with a media signal in a media signal processing system, the system including a media signal recorder, a computer, and an interface for communicating between the recorder and the computer, an improvement comprising automatically steganographically encoding media signal data with digital watermark data upon transfer to the computer.

31. The method of claim 30 which includes associating metadata in the recorder with a media signal captured in the recorder, transferring said metadata to the computer with the media signal, and associating said metadata in the computer with the digital watermark.

32. The method of claim 30 in which the digital watermark data permits detection of subsequent media signal alteration.

33. The method of claim 30 in which the encoding is performed by the computer.

34. A method of operating a media signal capture system, the system including a media signal capture device and a distinct computer with a user interface, the method including providing to the media signal capture device from said computer at least one data item to be steganographically encoded in a media signal captured by the media signal capture device, wherein the user interface of the computer is utilized to specify the data item.

35. The method of claim 34 which includes providing a steganographic link to the media signal capture device from the computer.

36. A method of maintaining a transaction history for media signal processing transactions on media signals, the method comprising:

maintaining a transaction history of a media signal stored on a networked device;

in response to receiving a transaction request to process a media signal stored on the networked device, updating the transaction history of the media signal by adding data about the transaction to the transaction history.

37. The method of claim 36 including:

associating the transaction history with the media signal through a link between the media signal and the transaction history.

38. The method of claim 37 wherein the link is a steganographic link embedded in the media signal.

39. A method for processing metadata of a media signal comprising:

embedding metadata steganographically in the media signal.

40. The method of claim 39 wherein the metadata in the media signal is encrypted.

41. The method of claim 39 wherein the metadata in the media signal is compressed.

42. The method of claim 39 wherein the metadata in the media signal includes a metadata digest of metadata stored outside the media signal.

43. The method of claim 39 wherein the metadata in the media signal includes a content signature.

44. The method of claim 39 wherein the metadata in the media signal includes a metadata signature.

45. The method of claim 39 wherein the metadata in the media signal includes a time stamp.

46. The method of claim 39 wherein the metadata in the media signal includes a location stamp.

47. The method of claim 39 including:

storing metadata of the media signal externally to the media signal;

wherein the metadata in the media signal and the metadata stored externally are related in a manner in which validity of the metadata can be evaluated by comparison.

48. The method of claim 39 wherein the metadata includes a link to metadata stored in an external database.

49. The method of claim 48 wherein the metadata stored in the external data base is searchable to find media signals based on attributes of the media signals stored in the metadata of the external database.

50. A method of electronic data searching comprising:

decoding a watermark from a first media signal;

using the watermark to access metadata about the first media signal stored in a metadata database accessible via a network, the metadata database having metadata for other media signals; and

using the metadata to search the database for related metadata of other media signals.

51. The method of claim 50 wherein the database is distributed in distinct metadata databases on two or more different computers on a network.

52. The method of claim 51 wherein information from the watermark is sent to a metadata router, which in turn, sends a request for information to a corresponding metadata database associated with the watermark information.

53. The method of claim 51 wherein a search request for the search is sent to a metadata router, which in turn, routes the search request to two or more different metadata databases.

54. The method of claim 50 wherein the related metadata found in the search is returned to a device that made the request for the search.

55. The method of claim 54 including:

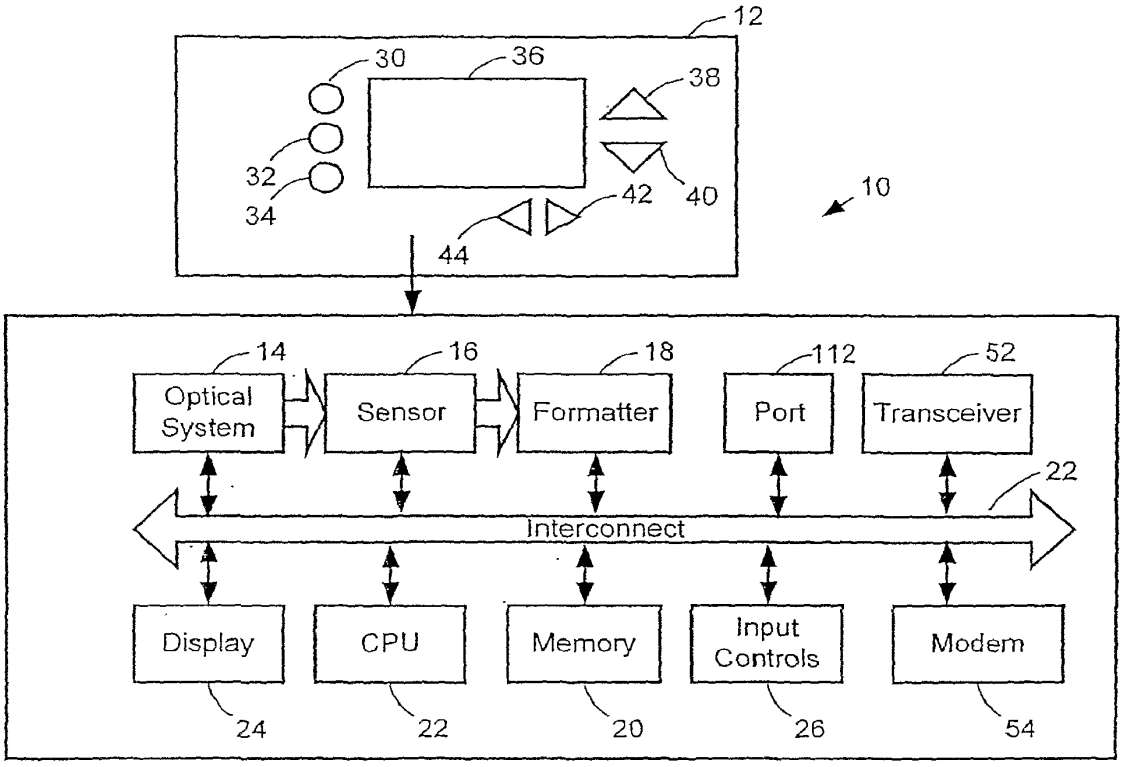
sending information from the watermark to a metadata router;

routing a search request for the search from the router to one or more different metadata databases;

wherein the related metadata is returned from two or more different metadata databases.

56. The method of claim 55 wherein the device that made the request for the search is also the device that decoded the watermark.

Fig. 1


12
30
36
38
32
34
42
40
44
10
14
16
18
112
52
Optical System
Sensor
Formatter
Port
Transceiver
22
Interconnect
Display
CPU
Memory
Input Controls
Modem
24
22
20
26
54

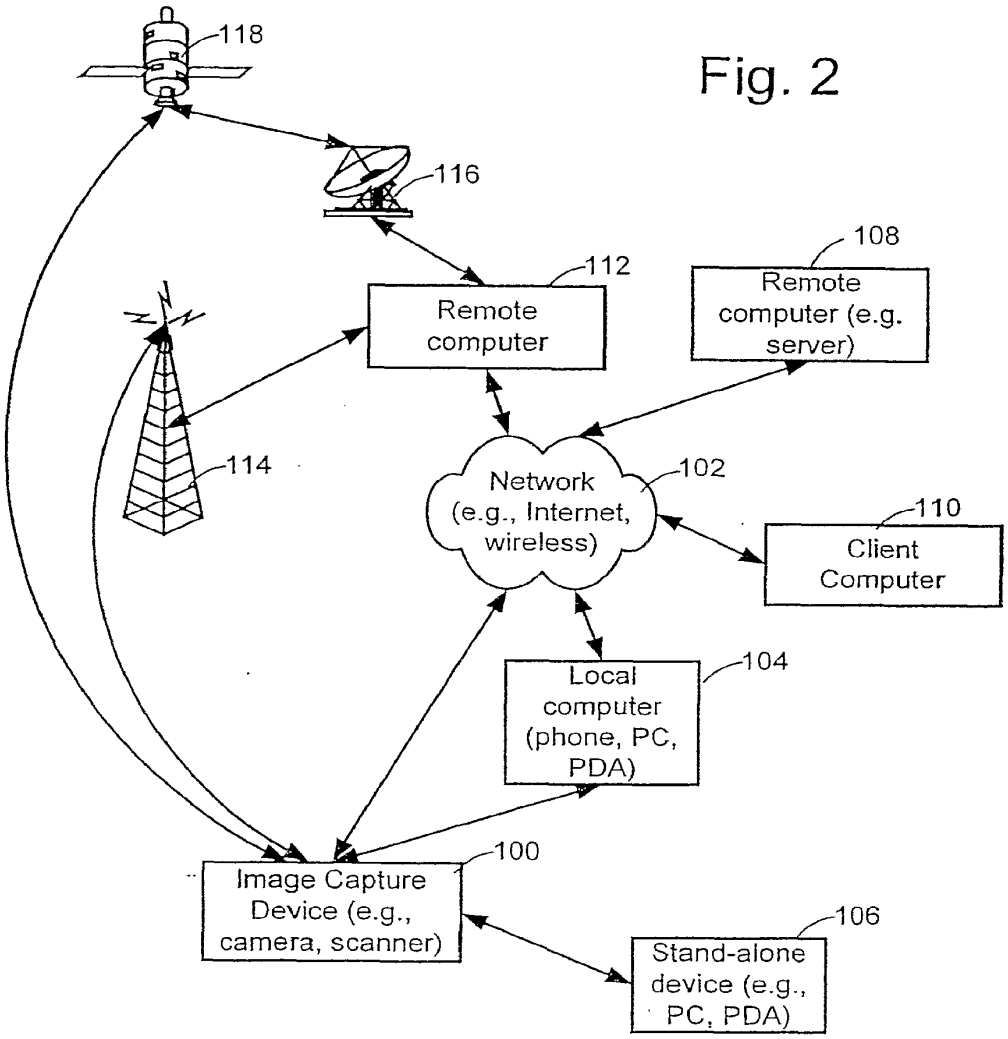

118
116
112
Remote computer
108
Remote computer (e.g. server)
114
Network (e.g., Internet, wireless)
102
110
Client Computer
104
Local computer (phone, PC, PDA)
100
Image Capture Device (e.g., camera, scanner)
106
Stand-alone device (e.g., PC, PDA)

Fig. 2

Fig. 3

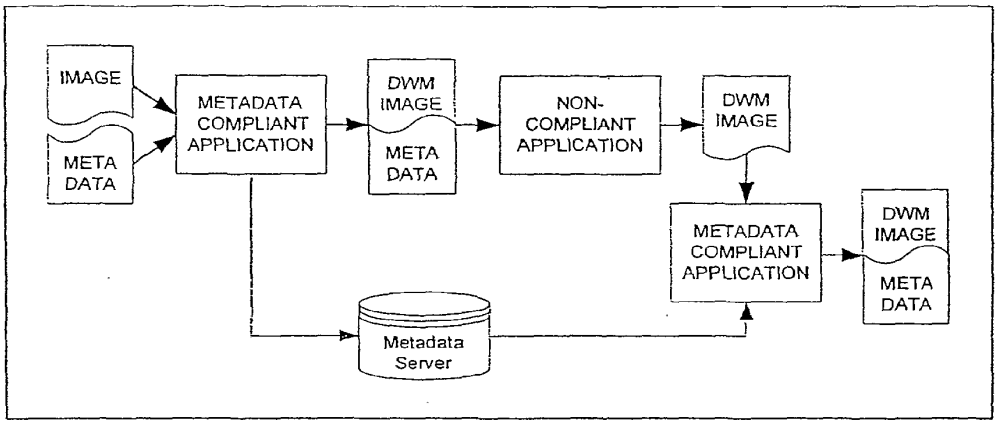
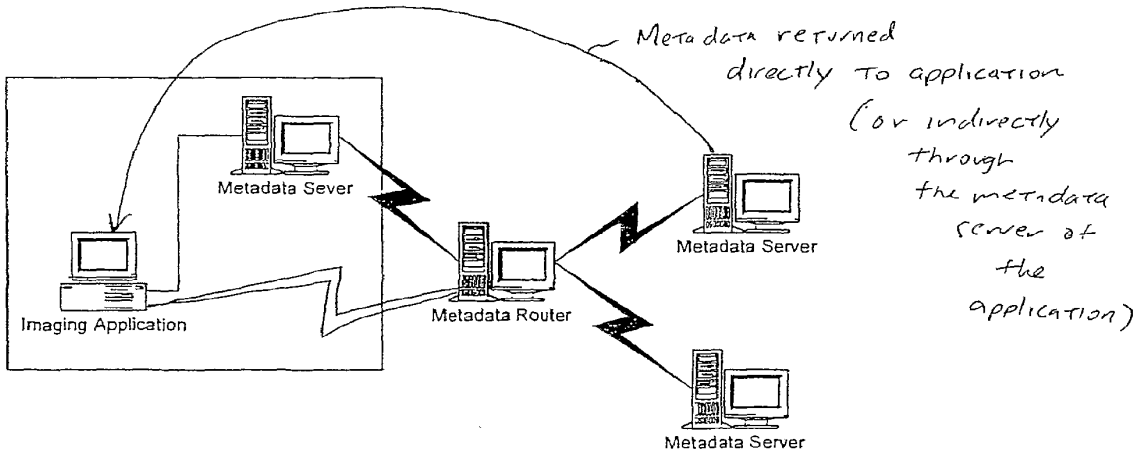

IMAGE
META DATA
METADATA COMPLIANT APPLICATION
DWM IMAGE
META DATA
NON-COMPLIANT APPLICATION
DWM IMAGE
METADATA COMPLIANT APPLICATION
DWM IMAGE
META DATA
Metadata Server

Fig. 4


Metadata returned directly to application (or indirectly through the metadata server of the application)
Metadata Sever
Imaging Application
Metadata Router
Metadata Server
Metadata Server

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/01043

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06K 9/00
US CL : 707/3, 707/6, 707/104

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 707/3, 707/6, 707/104

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 6,167,385 A (BEEK et al) 26 December 2000, col. 4, line 60 through col. 5, line 30.	1-56

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 02 MARCH 2001	Date of mailing of the international search report 10 MAY 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Mahmood Choobin Telephone No. (703) 306-5787

Form PCT/ISA/210 (second sheet) (July 1998)★

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G09G 5/00 — A1

(11) International Publication Number: **WO 99/01859**

(43) International Publication Date: 14 January 1999 (14.01.99)

(21) International Application Number: PCT/US98/13566

(22) International Filing Date: 29 June 1998 (29.06.98)

(30) Priority Data:

60/051,576	2 July 1997 (02.07.97)	US
60/073,967	6 February 1998 (06.02.98)	US

(81) Designated States: AU, CA, JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(71) Applicant *(for all designated States except US)*: IMIGE INCORPORATED [US/US]; 25159 N.E. Butteville Road, Aurora, OR 97002 (US).

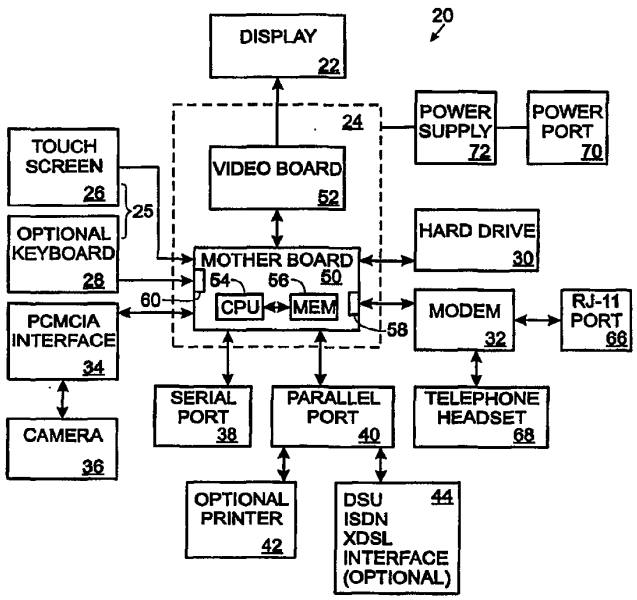
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: HAYHURST, Bill [US/US]; 25159 N.E. Butteville Road, Aurora, OR 97002 (US). WARD, Frederick, H. [US/US]; 13841 Tobiasson Road, Poway, CA 92604 (US). DABNEY, James, H. [US/US]; Suite B, 1366 Logan Avenue, Costa Mesa, CA 92626 (US).

(74) Agent: HUGHEY, Patrick, W.; Hancock Meininger & Porter LLP, 4370 N.E. Halsey Street, Portland, OR 97213 (US).

(54) Title: MOBILE TELECOMMUNICATION DEVICE FOR SIMULTANEOUSLY TRANSMITTING AND RECEIVING SOUND AND IMAGE DATA

(57) Abstract

A mobile telecommunication unit (20) provides two-way remote viewing of images and real time audio. The self-contained, portable unit (20) communicates directly with a similar unit at a remote location across POTS lines, cellular, ISDN, T-1, and satellite communication links. The unit (20) includes mass storage for archiving images. Input devices (25) for each unit include a digital camera (36) through a PCMCIA card, electronic stethoscope, telephone handset, speakerphone, external microphone, and serial and parallel ports. The output devices include a full color screen (22) for viewing local and received images and a speaker for audio output. A hard copy of images can be made by a video printer or desktop printer (42). Images can be uploaded to a PC.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

MOBILE TELECOMMUNICATION DEVICE FOR SIMULTANEOUSLY TRANSMITTING AND RECEIVING SOUND AND IMAGE DATA

Technical Field

The invention generally relates to a telecommunication device that allows remote consultation in a variety of fields such as medicine, real estate, insurance, engineering. More particularly, it allows an expert to take part in analysis of an event from a remote location by two-way transmission of sound and image data.

Background

In many industries, the ability to converse and share images with an individual located remotely can provide a great advantage. Communicating by phone is inadequate in many cases, and particularly in the medical industry, where it is critical to have visual information to make a thorough diagnosis. A device that could send visual information on the spot would save time, and money in shipping costs. Such devices exist today, but they are very expensive and typically communicate only between two fixed points.

Many industries in today's economy could take advantage of a portable and versatile device that could communicate still images and audio to remote locations without the need for a central unit. Today, an individual must physically visit a site, or send a hard copy of an image. A real estate agent must ship pictures across the country, consuming time and shipping costs. An insurance claims agent must send pictures to a central office to process claims. An engineer must physically visit a site to inspect problems.

The medical industry in particular may benefit from such device. A rural doctor must consult by telephone and describe the injury, usually unsatisfactorily, or ship x-rays or other diagnostic data, or even send the patient to the specialist. An Emergency Medical Technician must describe injuries to emergency room personnel. A doctor on-call must drive into the emergency room, not knowing specifics of an injury. A physician must wait for x-ray, MRI, or CT images to be shipped to an insurance company for authorization. All of this takes up valuable treatment time.

In recent years, medical costs have sky-rocketed. Driven by HMO's and other economic factors, efforts to decrease health care costs are being aggressively pursued. A device that transmits images of patient injuries in a matter of seconds to anywhere in the world would save expensive shipping costs of such images. More importantly, it would expedite the treatment of injuries, and offer access to specialists in geographic areas where it is not possible today.

Summary of the Invention

The invention provides an alternative solution that avoids the delay and high cost of shipping images and enables a user to provide a diagnosis from a remote location via simultaneous transmission of voice, image and possibly other data. Specifically, the invention provides a mobile telecommunication unit that sends audio and image information simultaneously and eliminates the cost and delay of shipping images and other diagnostic information. The device is portable, supports a variety of modes of telecommunication (e.g., POTS, cellular, ISDN, T-1, or satellite), and can send voice data and possibly other sounds simultaneously with image data.

One implementation of the invention is a portable, mobile telecommunication unit that is designed to transmit voice and still image data simultaneously to a compatible device on the other end of a telephone connection. One unit is placed into contact with a second, compatible device by a phone call. All controls, except for a power switch, are entered on virtual buttons on a touch screen. The telephone connection is made via POTS, or optional cellular, ISDN, T-1, or satellite. To capture an image, the user takes a picture with a digital camera provided with the unit. Through a camera interface, the digital camera transfers an image to the local unit. The local unit can then transmit the image to the remote unit.

In the course of capturing and viewing the image, the image data is modified somewhat to include fields for carrying text information, such as patient name, doctor, birth date, date of the image, and case notes (specific information concerning the patients medical condition).

The users at each location can talk to each other on the same telephone connection because the units transfer voice and image data to each other simultaneously. The user at the remote site can request, in real time, another view or a zoomed image. Consultation is much more accurate when both parties are viewing the same image and are able to converse. In this regard, discrete pointers or tags may be instantaneously added to the image by one or both parties (hence transmitted to and viewed by the other party) to direct the conversation to selected features of the image. The pointer information is generated and transmitted in a way such that the position of the pointer relative to the remainder of the image will be constant irrespective of other changes in the view of the image, such as panning or zooming.

To further focus the conversation about an image, pointers placed on an image at remote unit will have a different appearance (such as by coloring) than pointers generated on a local unit. Thus, both parties have an immediate graphical indication of which pointer was generated by which party.

The pointers may be instantaneously removed from the image or stored with the image for future reference. In this regard, the above mentioned case notes can refer to pointers added to and saved with the image. This correlation between the text and image information speeds the review and comprehension of the patient information.

The unit at either end of the telephone connection can archive all the pictures transferred or selected images on the internal hard drive. Software executing in a unit controller enables the user to categorize images on the hard drive into folders unique to the individual. When a telephone connection with a remote system is established, and images are to be sent, the receiving system is checked for an existing folder for the individual. If it is not found, one is created. As noted, information such as patient name, time, date, and referring physician is sent with the image.

Every image collected from, for example, a digital camera is provided with a unique filename that includes a multi-digit number and a code identifying the particular unit. Thus, there is no likelihood that two different images residing in

one unit will have the same filename. Similarly, the use of the code that identifies the particular unit ensures that different images from two machines will not, by chance, end up with the same filename. It will be appreciated that the elimination of confusion as to image filenames is particularly important when the system is used, for example, for diagnostic and treatment procedures.

Either user can make a hard copy of the information with a printer accessory. One or both of the users can view the images on an external monitor, and listen on an external speaker. Either user can use a phone handset, or a hands-free speakerphone. An external microphone can be used, or an electronic stethoscope can be plugged into hear a patient's heartbeat or breathing. An optional software enhancement can send and display EKG data.

Another application is in the real estate industry. For example, a real estate agent can use the mobile telecommunication unit to give a tour of a home on the East Coast to a prospective buyer on the West Coast. The agent can give a walk-through, room-by-room, showing different angles requested by the buyer. The agent can then travel outside to show the exterior and the neighborhood. This will allow a more thorough tour than would a small packet of snapshots, and will be tailored exactly to the buyer's request.

Yet another application of the invention is in the insurance industry. An insurance claims agent can survey damage, and immediately send the information to the central office. This allows accurate, on-the-spot claim processing, saves shipping costs, and provides more effective customer service.

In yet another application, an engineer could check the progress of a project across town or across the country without having to waste time traveling to the location. Viewing the project would allow a more accurate analysis than a verbal description over the phone. It would save unnecessary trips, time, and money.

The invention can provide a significant improvement in providing medical services. A doctor in a rural location could consult with a specialist in another region, providing service to a community not presently available. The patient

may not have to be transported hundreds of miles for treatment that could have been performed in their hometown, saving thousands of dollars in ambulance fees. An emergency medical technician could consult with the emergency room doctor, and start treatment on the way to the hospital, saving the most valuable time in trauma treatment. A doctor on call could diagnose the patient from home, possibly saving unnecessary trips to the emergency room. Alternatively, the doctor could instruct the operating room personnel on special needs for a special procedure, saving valuable treatment time. A physician could send an image to an insurance company for instant approval, instead of waiting the standard two weeks now allocated.

The invention could be used in other industries as well, such as geologic survey, business consulting, advertising, and visual consulting of all sorts.

Additional features and advantages of the invention will become more apparent from the following description of the preferred embodiment.

Brief Description of Drawings

Fig. 1 is a block diagram illustrating an embodiment of a mobile telecommunication unit designed according to the invention.

Fig. 2 illustrates a perspective view of one implementation of the mobile telecommunication unit shown in Fig 1.

Fig. 3 illustrates a top plan view of the mobile telecommunication unit of Fig. 2.

Fig. 4 illustrates a front elevation view of the mobile telecommunication unit of Fig. 2.

Fig. 5 shows a side elevation view of the mobile telecommunication unit of Fig. 2.

Fig. 6 is a flow diagram illustrating the operation of the unit at start-up.

Fig. 7 is a flow diagram illustrating the operation of the unit when the user activates the send module from the start up screen.

Fig. 8 is a flow diagram illustrating the operation of the connect module.

Fig. 9 is a flow diagram illustrating the operation of the address book module.

Fig. 10 illustrates the operation of the system when the user activates a module for choosing settings of the unit from the start-up screen.

Fig. 11 is a flow diagram illustrating the operation of the system when the user activates the view images module.

Fig. 12 is a flow diagram illustrating the operation of the system when the receive module is activated.

Fig. 13 is a flow diagram illustrating the operation of the delete module.

Fig. 14 is a flow diagram illustrating the operation of the archive module.

Fig. 15 is a flow diagram illustrating the operation of the zoom module, which enables a user to manipulate an image on the display.

Fig. 16 is a flow diagram illustrating the operation of the system while it is in idle mode.

Best Modes for Carrying Out the Invention

Fig. 1 is a block diagram illustrating an implementation of a mobile telecommunication unit 20 designed according to the invention. The unit 20 includes a display 22, a unit controller 24, a user input device 25 (touch screen 26, and optional keyboard 28), a secondary storage device (hard drive 30), and a modem 32. The unit 20 also includes a number of input/output devices including a camera interface 34 for connecting a camera 36 to the unit controller 24, a serial port 38, and a parallel port 40. The parallel port enables a variety of devices to be connected to the unit including a printer 42, or an interface 44 for ISDN, DSL (Digital Subscriber Line), or digital modem.

The unit controller 24 is comprised of a motherboard 50 and a video board 52 for controlling the display 22. A central processing unit (CPU) 54 and local memory unit 56 are mounted to the motherboard 50, which is implemented using an ISA/PC 104 board from Advanced Computer Solutions, Inc. The CPU 54, an 80/486-DX4 based embedded microcontroller, plugs into the motherboard 50 and

interfaces with the local memory unit 56 via bus circuitry on the motherboard. The local memory unit 56 includes 640K of base memory and an additional 8 M of extended memory. The motherboard 50 also includes a serial interface 58 used to connect the modem 32 to the CPU and memory.

The video board 52 in the unit controller 24 controls the display 22 in response to control and data signals from the motherboard 50. The video board 22 includes a 512K frame buffer and is implemented using an MMX-VFPII from Ampro.

The display 22 is a high bright 35.5-cm color active matrix LCD. It has 640x480 resolution, 256K colors, and includes a cold cathode fluorescent tube (CCFT) back light. The display is a commercially available LCD device, and is specifically an NL 6448AC33-18 display from NEC.

The user-input device of the unit 20 is a touch screen 26 and is implemented using an E2741HL-683 touch screen and an E271-2210 touch controller from EloTouch Systems. Optionally, the user can connect a full sized keyboard 28 to the motherboard 50 via a standard keyboard interface 60.

The secondary storage device in the unit 20 is a hard disk drive 30. The hard drive 30 is connected to the motherboard 50 via a hard disk board. The specific board in this implementation is part number 950019 from Advanced Computer Solutions, Inc.

The modem 32 is a modular, internal device that plugs into the motherboard via the serial interface 58. The specific type of modem in the unit is an AM3314IVSP from Amquest. The modem supports 33,600 BPS maximum, and can transfer voice and data simultaneously. The modem is connected to a standard RJ-11 telephone connector 66 that connects the modem and telephone handset to a standard telephone line.

The unit 20 has a telephone operator interface that includes a virtual telephone keypad, and telephone handset 68. The virtual telephone keypad is controlled in software and displayed as an array of buttons that emulate a conventional telephone keypad. The telephone handset 68 is a standard

earphone/microphone device used to transmit and receive audio data. The telephone handset plugs into the modem 32, which, in turn, controls simultaneous voice and data transmission over a telephone line.

To supply power to the unit 20, the user plugs a conventional 120-volt AC power source into the power connector 70. A power supply 22 in the unit converts the input power into a power signal compatible with the electronic devices in the unit 20. In this implementation, the power supply is a BN330-3 available from Tri-Mag.

To operate the device, a user enters input commands via virtual buttons displayed on the touch screen 26. The layout of the virtual buttons include a virtual keyboard and a virtual telephone keypad that enable the user to place and receive calls just like a conventional telephone.

To enter image data, the user captures a still image with the digital camera 36. The digital camera transfers the image via the PCMCIA interface to the unit controller 24. Executing image-processing software, the CPU processes the incoming digital image data and issues control signals to the video board to display the image on the display 22. The image processing software also enables a user to instruct the CPU to scale an image and archive the image on the hard drive 30 by entering commands via the touch screen or an optional keyboard.

In a preferred embodiment, the format of the image data is changed to allow the presence of the above mentioned text information (patient name and the like). To this end, a fixed-length header is inserted at the beginning of the image file provided via the PCMCIA interface. The header contains a number of data fields for patient information, which will be displayed with the image(s). Each of the fields contained in the header is prefaced with a length record, which allows the underlying software to dynamically change an internal field length should this become necessary.

Moreover, one of the data fields identifies the file as one that is valid with the system of the present invention. Thus a level of security is introduced

because the image/patient-information file can be opened only with a unit that processes in accordance with those of the present invention. That is, other viewers, etc. will not recognize the format of the image/patient-information file.

It is noteworthy here that the underlying software also permits conversion of the image data back to the format originally received (by stripping off the added text and identification data) so that the image can be recognized and used by other viewers or image processing systems.

As noted above, every image collected from the digital camera is provided with a unique filename that includes a multi-digit number and a code identifying the particular unit. Thus, there is no likelihood that two different images residing in one or more units will have the same filename. Specifically, whenever file activity concerning previously unnamed (by the present system) files occurs – such as copying the image data files from the PCMCIA card to the system's storage memory- the CPU, under the control of the system software, refers to the last-used file number saved on the system and counts up as necessary to generate a filename for each new, discrete image. That number, preferably a hexadecimal (five digit's worth), is coupled to the unit's unique identifying code and used to name the particular image file. The new file number is saved in the system for look-up when the next, unnamed image files are acquired.

The CPU executes modem control software that enables the user to place a call to a remote location and then transmit voice and image date simultaneously via the phone line. The phone connection is typically made via a conventional POTS line, but also can be made via a cellular ISDN, T-1 or satellite communication link.

The modem control software performs a variety of call control and data transmission tasks, including packaging and unpackaging image data so that it can transmitted via a phone line and reconstructed. When the telecommunication unit is in the receive mode, it unpackages image data from the phone line and progressively displays the image on the display. The modem separates image data from voice data and transfers the image data to the unit controller. Image processing software executing in the CPU then renders the

image for display via the frame buffer in the video board. The modem sends incoming voice signals to the telephone handset 68, which, in turn, converts the voice signal into an audio signal.

Having described the internal structure and operation of the telecommunication unit, we now turn to the external structure of the unit.

Fig. 2 illustrates a perspective view of one implementation of the mobile telecommunication unit 20 shown in Fig 1. The mobile telecommunication unit 20 is enclosed in a portable carrying case. Specifically, the enclosure 122 is a modified 103 C-SI briefcase manufactured by Zero Halliburton. The approximate size of the briefcase is 45.7 cm by 33.0 cm wide by 15.2 cm deep. The interior compartment of the briefcase has a storage space 124 for a digital camera 126 and an additional storage space 128 for connector cables.

The interior compartment also includes a variety of parts for mounting the electronic devices shown in Fig. 1 securely inside the briefcase 122. A chassis 130 is mounted to the bottom panel 132 of the briefcase. A display connector plate is used to mount the display to the chassis. A shield plate shields the electrical components connected to the back of the display from the display. Finally, a secure plate is used to mount the electrical components to the back of the display.

The user interface and other electronic components in the unit 20 are implemented in an integrated mounting structure that includes a display assembly 140 and a series of stacked boards mounted to it. The display assembly is comprised of a touch membrane 150, fastened adjacent to the viewing surface of an LCD display 152. The motherboard 154 and hard disk board 156 are mounted in a stacked configuration on one side of the back of the display. The PCMCIA interface board 160 and modem 162 are mounted in a stacked configuration on the other side of the back of the display. The display 152 and the components mounted to it are fixed inside the enclosure. The power supply 170 of the unit 20 is mounted to the bottom panel of the enclosure and sits underneath the display assembly.

The unit is also equipped with a telephone, which includes a telephone handset and a speakerphone. The telephone includes an extra audio input for an electronic stethoscope. The telephone plugs into the modem through a telephone line connector.

Fig. 3 illustrates a top plan view of the mobile telecommunication unit 20. The top view shows the position of the camera compartment relative to the display. Each of the three-digit reference numbers shown in Fig. 3 correspond to the same components as in Fig. 1 where the Fig. 1 reference numbers have the same digits as the last two digits of the Fig. 3 numbers.

Fig. 4 illustrates a front elevation view of the mobile telecommunication unit 20. This view shows the stacked configuration of the mother board 154 and hard drive 156 on one side of the display assembly, and the stacked configuration of the PCMCIA card 160 and modem 162 on the other side of the display assembly.

Fig. 5 shows a side elevation view of the mobile telecommunication unit 20. This view more clearly illustrates how the touch membrane 150 and other boards are connected to the display 152. The touch membrane 150 is mounted on the top of the display 152 via conventional fasteners 180a-b. The motherboard is mounted to the back of the display via fasteners 182a-b. The PCMCIA board 160, and modem 162 are mounted to the back the display via fasteners 184a-b.

The power supply 170 is mounted to the bottom panel 132 of the case 122. A power connector 190 and power switch 192 are located adjacent to the power supply 170 on the side of the unit 20.

In addition to the unique features of the preferred hardware configuration, the software contains many distinctive attributes. The software executing on the unit includes the user interface as well as routines used to establish connections, transfer audio and image data, perform file management, encode and decode image data files, and perform image processing functions.

An objective of the user interface design is to make the unit easy to use and to avoid the need for extensive training. To achieve this goal, a menu driven software package was developed to run on a DOS based platform. All functions of the user interface are accessible though virtual buttons created by the software. Intuitive menu choices allow inexperienced users to utilize the power of the system fully. An on-line help system is also included to guide users though any problems they might encounter.

Fig. 6 is a flow diagram illustrating the operation of the unit at start-up. When power is turned on 201, the system displays a logo screen 202, which starts an initiation process. The user is asked 203 for a Personal Identification Number, PIN. If the PIN is correct, the system displays the start up screen 204. If a user forgets the PIN, then a special ten-digit PIN can be entered 205 to reset the PIN to 0000. The PIN requirement can be turned off in the settings module described below with reference to Fig. 10, 252. The start up screen displays virtual buttons for send 207, connect 208, address book 209, settings 210, full screen 211, view images 212, and automatic receive 213. When the user selects one of the buttons, the system activates the corresponding module.

Fig. 7 is a flow diagram illustrating the operation of the unit when the user activates the send 214 module from the start-up screen. Images can be selected from the archive (e.g., a file system for the hard disk) using the view images module shown in Fig. 11. If the system is connected to a remote system 215, the selected images 221 are sent to the remote unit 222. If the system is not connected to a remote system 215, the connect module is activated 225 to send images 226.

Fig. 8 is a flow diagram illustrating the operation of the connect module. The connect module is activated 227 by the virtual button for the connect module 208, or automatically through send (Fig. 7), or view (Fig. 11). The phone number to dial can be selected in one of two ways. First, a virtual telephone keypad 228 can be displayed 229 and activated to enter the number manually 230. The system then dials the number as shown in function block 233. Second, a number can be selected from an internal address book 231. The address book module is

then activated 232 as shown in Fig. 9. When the number is returned from the address book, the connect module executes a routine to instruct the modem to dial the number 233.

Fig. 9 is a flow diagram illustrating the operation of the address book module. The address book module 234 is activated from the start up screen, or the connect function. The user can select the system address book (shown as IMIGE) 246, a personal address book 235, or can return to the previous screen. The system address book is automatically updated monthly when the system is logged onto a bulletin board to report minutes of usage, and receive software upgrades. If the user selects a name from the list 247, the user is given an option to store the name in the personal address book 235. The system is connected 248, 249 to the remote system selected from the system address book.

If the user selects the personal address book 235, the system displays a list of names 236. The user then has the option to create a new entry 241, exit 243 to the start of the address book 234, or select a name from the list 237. If the new entry 241 is selected, the user is prompted to fill in fields such as the contact's name, phone number, and address. If the user selects a name 237, the system displays the properties of the contact 238. The fields can then be edited 244, 245, or a connection can be established 239, 240.

Fig. 10 illustrates the operation of the system when the user selects the setting module 251 from at the start-up screen. Presently, there are two features for which the settings can be changed: 1) auto answer and 2) change PIN. More features can be added during the monthly update. If the user selects auto answer 264 to change the feature settings, the system gives two options: one to disable auto answer 265, and another to set the number of rings before answering 267. If the change PIN 252 option is selected from the settings screen 251, there are two options, disable PIN 253, or set new PIN 258. If the user selects the disable PIN 253 feature, the user is prompted to input the present PIN 254. If the user has forgotten the PIN, then the special ten digit PIN is entered, the PIN function is turned off 256, and the system returns 257 to the settings screen 251.

If the user selects the option to set a new PIN 258 from the change PIN branch 252, the user is prompted for the current PIN 259. The special ten-digit PIN can also be entered here. To verify the PIN, the user is prompted to enter the new pin twice and each time the PIN is checked to make sure it is correct 260-262. If it is correct, the system stores the new PIN as the current PIN 263.

Fig. 11 is a flow diagram illustrating the operation of the system when the user activates the view images module 269. This module enables a user to view images from an archive 272 on the hard disk, a PC card 271, or an auxiliary device 287. If the archive is selected 270, the user can then select a patient folder 273. When a user selects a folder, the system first displays thumbnail images 274. If the user selects images from a PC card 271 or an auxiliary device 287, the user can first select thumbnail images 274. From the thumbnails, the user can select an individual image 275. When the user selects a thumbnail, the system displays a full screen view of the selected image 276. As noted above, the originally received image is modified to include patient information. Thus, the full screen image will include the information, preferably located in a corner of the screen. Alternatively, the patient information can be hidden from the view, so that the entire screen can be devoted to display of only the image. The user can then choose to zoom 277, send 279, connect 281, delete the image 287, or archive the image 285.

As shown in Fig. 11, at 276, the system displays the image along with the virtual buttons described above. Two of these buttons, which may be labeled "POINT" and "UNPOINT" are responsive to the user's touch to carry out the pointer or tag functions described earlier. The pointers are dynamically generated for the active file. Thus, the operator selects the POINT button, which prepares the system to treat the next touch of the screen as a location on the image where the user desires a new pointer. The pointer may be any suitable icon.

The system assigns a new, unique value or identifier to display as or with the pointer, such as a letter "A." Once the screen is touched, the user's unit generates a packet of data comprising the following: 1) the screen coordinates (x,

y) in pixel units of the selected (touched) pointer location, 2) the zoom factor employed in the user's view, 3) the x and y offsets associated with the image database (the real image is always larger than the display area, so there is re-mapping between the screen and the image –this allows panning and zooming), 4) the filename of the active image, and 5) the current value of the pointer.

With this information the pointer can be dynamically repositioned (that is, maintain its proper relative positional relationship in the image) irrespective of whether the viewer pans or zooms to change the view of the image.

The data packet is instantly provided to the remote unit (that is connected to the user's, local unit) so that that unit can replicate the zoom factor, pan viewpoint, pointer value and location on the correct image. As noted above, a received pointer will, preferably, have a different color or appearance as compared with one generated on the receiving machine.

After the UNPOINT button is touched, the system removes the last-added pointer from the local and remote units. Subsequent touches of the UNPOINT button sequentially removes the remaining pointers, newest ones first.

Fig. 12 is a flow diagram illustrating the operation of the system when the receive module 288 is activated. The remote unit only activates this module when an image or group of images is sent to the local system. The system checks a patient name of the received image 289. If a patient folder does not already exist 290, the system creates one 291. Next, the system stores the image in the existing or the newly created folder 292. If more images are to be received 293, steps 289-293 are repeated. When the remote connection is terminated the system returns to its prior state 294.

Fig. 13 is a flow diagram illustrating the operation of the delete module 295. When the delete module is activated, three options are possible: delete an image on the PC card 296, delete an image from the archive 297, and exit 298 to the prior screen. Thumbnails are shown 300 from the PC card 296 or the archive 297. The user can exit (301, 302) the delete 295 module at this time. If the user wishes to delete an image, he or she selects the images to delete 303. The user

is asked to select delete again to verify that the user wants to delete the image 304-306. The image is deleted 307 if the user selects the delete option and then confirms the delete operation as shown in blocks 304 and 306.

Fig. 14 is a flow diagram illustrating the operation of the archive module 308. When the user activates the archive module, the system displays a screen that enables the user to create a new patient folder 309, save images to an existing patient folder 312, or exit 310 to the previous screen 311. If the user chooses to create a new patient folder, the system prompts the user for patient information 309 such as, name, birth date, and referring doctor. If the user chooses to save an image to an existing folder 312, the folder is selected 312 and opened 313, and the image is saved 314.

Fig. 15 is a flow diagram illustrating the operation of the zoom module 315, which enables a user to manipulate an image on the display. The zoom module can be activated when an image is displayed 316. The zoom module provides four options: zoom in 317, zoom out 320, view full screen 323, and exit 326 to previous screen. If the user requests the zoom in function 317, the system prompts the user to touch the center of the zoom 318. In response, the system scales the image and displays the zoomed image 319. This can be repeated to magnify the image. The user can also choose to reduce the image 320. In response, the system reduces the image and displays the reduced image 321. The user can also choose to display an image so that it occupies the full screen 323. If the user selects the full screen option, the system displays the present image 324 until the user makes a vertical sweep 325 of the touch screen.

Fig. 16 is a flow diagram illustrating the operation of the system while it is in idle mode 328. An idle module executes on the system when it is in idle mode. Idle mode is activated any time that there has not been a touch of the screen or an activation of the unit by a remote system for a predetermined period of time, e.g., five minutes. When idle mode 328 is activated, a logo screen 329 is displayed for thirty minutes 330. After thirty minutes the screen is deactivated and turns black 331 saving on power consumption. Any time the screen is

touched or a remote system activates the unit 332, it reverts back to the screen displayed prior to idle mode 213.

The software is not limited to functions accessible to the user. An internal timer keeps track of time connected to a remote system. Every month the system automatically calls a bulletin board and reports the minutes of use. The system has been designed for easy software upgrade. New software can be implemented by PC card, remote access through the modem, or during the monthly connection. Any system wide upgrades will be transferred to the remote units during the monthly connection. The system can be set up to make an automatic connection over night to save on long distance charges. All images are transferred in an encrypted file format, providing a level of encryption that does not allow viewing of the images except for another system unit. The system encrypts image files by encoding a text file including information about the image, such as a patient name, doctor, birthdate and date of the image, in an image file as described above.

While the invention is described with reference to a specific implementation, it should be understood that the scope of the invention is not limited to this implementation. A variety of types of input devices and display devices can be used to implement the user interface. In addition, the software features and implementation can vary as well.

In view of the many possible embodiments to which the principles of our invention may be applied, it should be recognized that the illustrated embodiment is only a preferred example of the invention and should not be taken as a limitation on the scope of the invention.

Claims

1. In a system that displays an image on a local display unit and on a remote display unit, which local and remote display units are used and observed by a respective local user and remote user, a method of identifying portions of the displayed images, comprising the steps of:

displaying on the local unit a first local icon at a location on the locally displayed image, which location being selected by the local user; and

transmitting to the remote user information for generating on the remotely displayed image a first remote icon corresponding to the first local icon such that the first remote icon is displayed on the remotely displayed image at the location on the image selected by the local user.

2. The method of claim 1 further comprising the step of providing the first remote icon with an appearance indicating that the location of the first remote icon was selected by the local user and not the remote user.

3. The method of claim 1 further comprising the steps of:

providing both the local and remote units with means to change the size of the remotely and locally displayed images by zooming; and

including in the information transmitted to the remote user data representing the size of the displayed local image thereby to permit the first remote icon to be displayed on the remote image at the location selected by the local user irrespective of differences in the size of the image displayed on the remote and the local units.

4. The method of claim 1 further comprising the steps of:

providing both the local and remote units with means to display selected portions of the remote and local images by panning; and

including in the information transmitted to the remote user data representing the location of the first local icon relative to a portion of the image that is common to both the local and remote image thereby to permit the first remote icon to be displayed on the remote image at the location selected by the

local user irrespective of differences in the portions of the images selected for display on the remote and the local units.

5. The method of claim 1 further comprising the steps of:

providing both the local and remote units with means to display two or more images at a time and for selecting one of the two or more images on which to display a first local icon; and

including in the information transmitted to the remote user data representing the one of the displayed two or more images on which the first local icon is displayed.

6. The method of claim 1 further comprising the steps of:

providing means for displaying on the local and remote units text information for display with the displayed image;

including in the information transmitted to the remote user data representing text information for display; and

associating the text information with the first local icon, thereby to associate that text information with the first remote icon.

7. The method of claim 1 further comprising in addition to the displaying and transmitting steps the step of removing from the local unit the displayed first local icon; and

transmitting to the remote user information for removing the first remote icon from the remotely displayed image.

8. The method of claim 1 further comprising the steps of:

displaying on the local unit a second local icon at a location on the locally displayed image, which location being selected by the local user;

assigning to the second local icon an appearance unlike that of the first local icon; and

transmitting to the remote user information for generating on the remotely displayed image a second remote icon corresponding to the second local icon such that the remote icon is displayed on the remotely displayed image at the

location selected by the local user.

9. The method of claim 1 including the steps of:
linking the local and remote units via a telecommunications system; and
sending voice data simultaneously with the information for generating the first remote icon.

10. The method of claim 1 including the step of packaging the local unit as a portable device connectable with more than one type of telecommunications system.

11. The method of claim 1 including the step of storing on the remote unit information representative of the remotely displayed image and first remote icon, thereby to enable later display of that image with the first remote icon.

12. The method of claim 1 further comprising the step of providing on the local unit a touch screen for permitting the local user to touch the local unit for selecting the location of the first local icon.

13. The method of claim 12 further comprising the step of displaying on the local unit a virtual button that, once touched, identifies a subsequent touch of the touch screen by the local user as the location selected for the local icon.

14. The method of claim 7 further comprising the step of providing on the local unit a touch screen for permitting the local user to touch the local unit for removing from the local unit the displayed first local icon.

15. The method of claim 14 further comprising the step of displaying on the local unit a virtual button that when touched by the local user is identified as a command for removing from local unit the displayed first local icon.

16. The method of claim 1 further comprising the steps of:
displaying on the remote unit a third remote icon at a location on the locally displayed image, which location being selected by the remote user; and
transmitting to the local unit information for generating on the locally

displayed image a third local icon corresponding to the third remote icon such that the third local icon is displayed on the locally displayed image at the location on the image selected by the remote user.

17. The method of claim 16 further comprising the step of providing the third remote icon with an appearance indicating that the location of the third remote icon was selected by the remote user and not the local user.

18. An image transmission and reception system comprising:
a local unit including:
an image-capturing device for capturing an image;
a local display device connected to the image-capturing device and operable for displaying the captured image;
a transmitting device for transmitting the image substantially simultaneously with voice data over a telecommunications system;
a case for enclosing and rendering portable the image-capturing device, the local display device, and the transmitting device; and
a remote unit, including:
a receiving device for receiving the image and voice data transmitted by the transmitting device;
a remote display device for displaying the image transmitted by the transmitting device; and
an audio device for providing audio signals corresponding to the voice data transmitted by the transmitting device.

19. The system of claim 18 wherein the remote unit further comprises:
an image-capturing device for capturing an image;
the remote display device being connected to the image-capturing device and operable for displaying the captured image;
a transmitting device for substantially transmitting the image substantially simultaneously with voice data over a telecommunications system; and
a case for enclosing and rendering portable the image-capturing device, remote display device, and transmitting device of the remote unit.

20. The system of claim 19 wherein the local and remote image-capturing devices are digital cameras and wherein the system further includes means for assigning to each captured image an identifier that specifies which one of the local and remote image-capturing devices generated the image.

5

Fig. 1

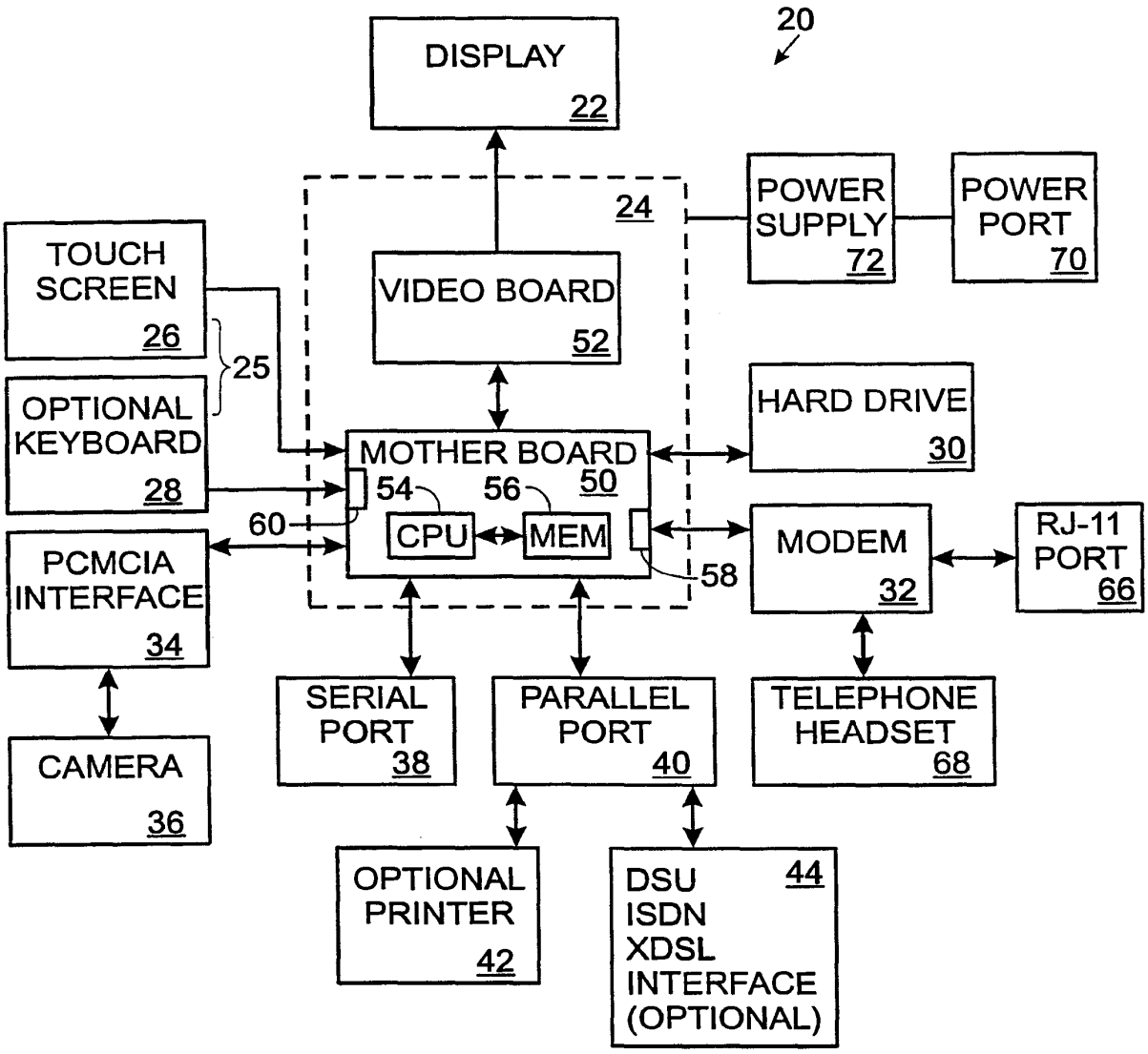

20
DISPLAY
22
24
POWER SUPPLY
72
POWER PORT
70
TOUCH SCREEN
26
25
VIDEO BOARD
52
OPTIONAL KEYBOARD
28
HARD DRIVE
30
MOTHER BOARD
50
54
56
60
CPU
MEM
58
PCMCIA INTERFACE
34
MODEM
32
RJ-11 PORT
66
SERIAL PORT
38
PARALLEL PORT
40
TELEPHONE HEADSET
68
CAMERA
36
OPTIONAL PRINTER
42
DSU ISDN XDSL INTERFACE (OPTIONAL)
44

Fig. 2

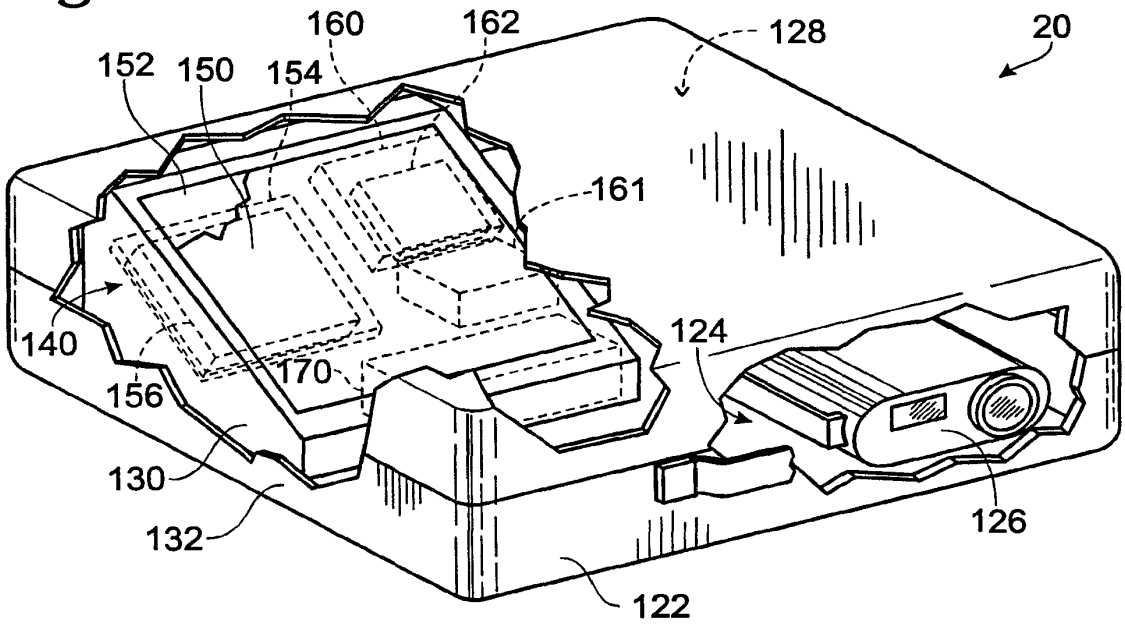

160
162
128
20
152
150
154
161
140
170
124
156
130
126
132
122

Fig. 6

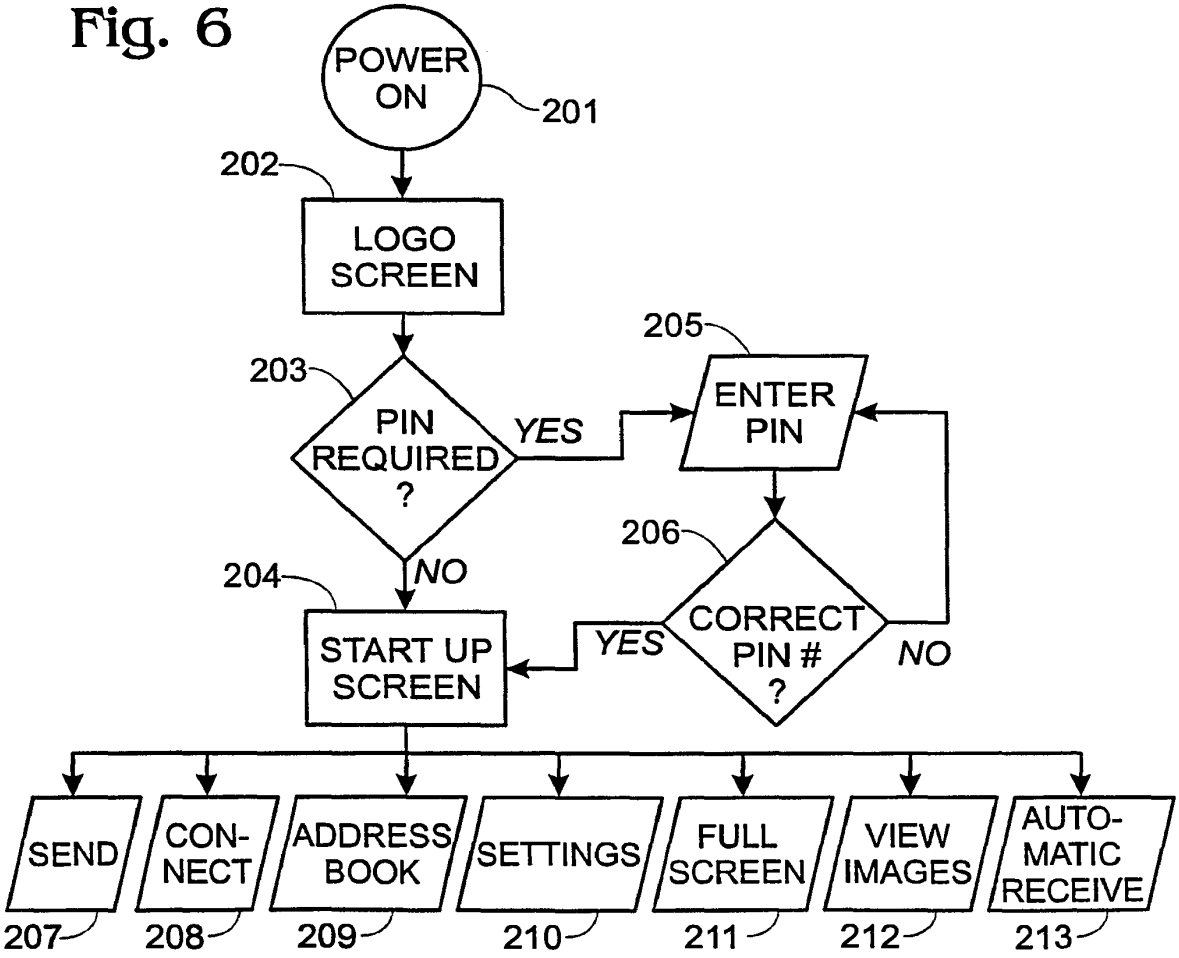

POWER ON
201
202
LOGO SCREEN
205
203
PIN REQUIRED ?
YES
ENTER PIN
206
NO
204
CORRECT PIN # ?
YES
NO
START UP SCREEN
SEND
CON-NECT
ADDRESS BOOK
SETTINGS
FULL SCREEN
VIEW IMAGES
AUTO-MATIC RECEIVE
207
208
209
210
211
212
213

Fig. 3

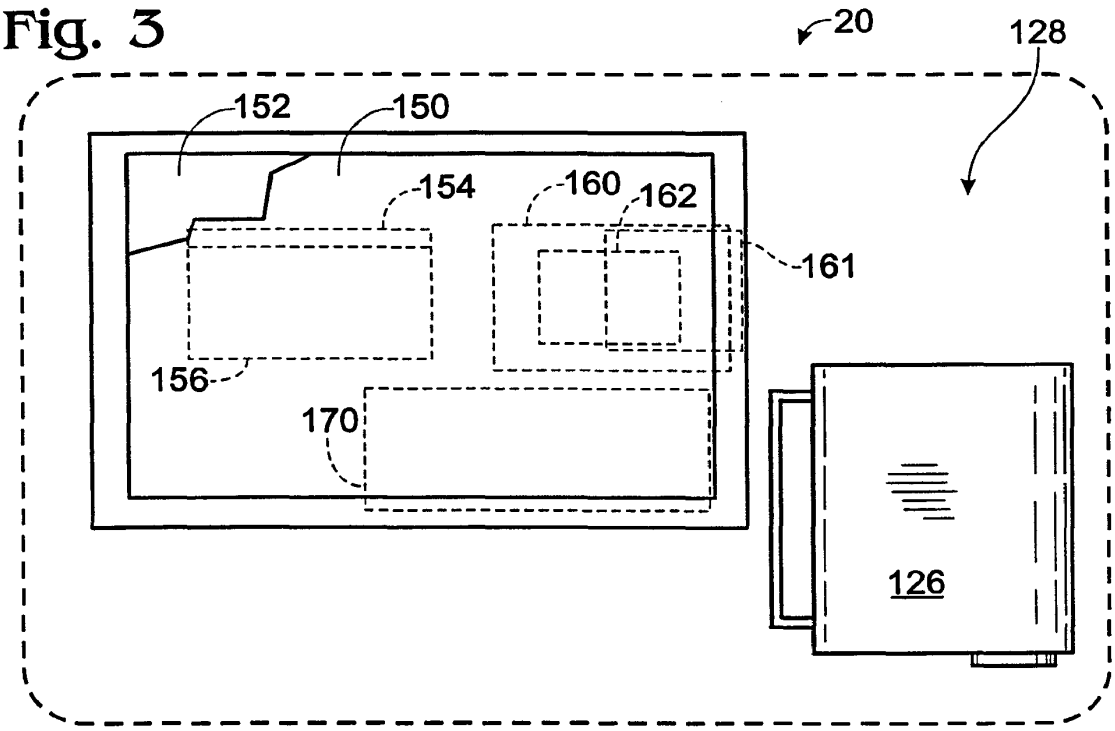


Fig. 4

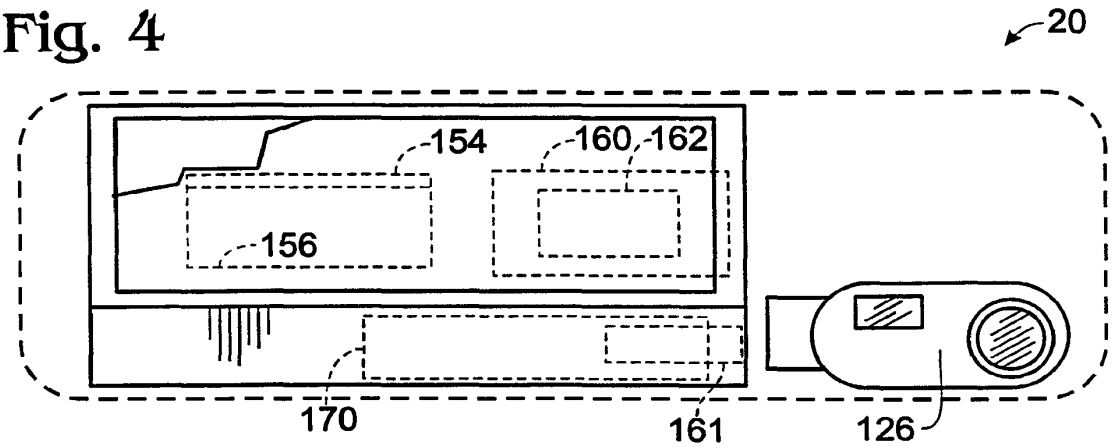


Fig. 5

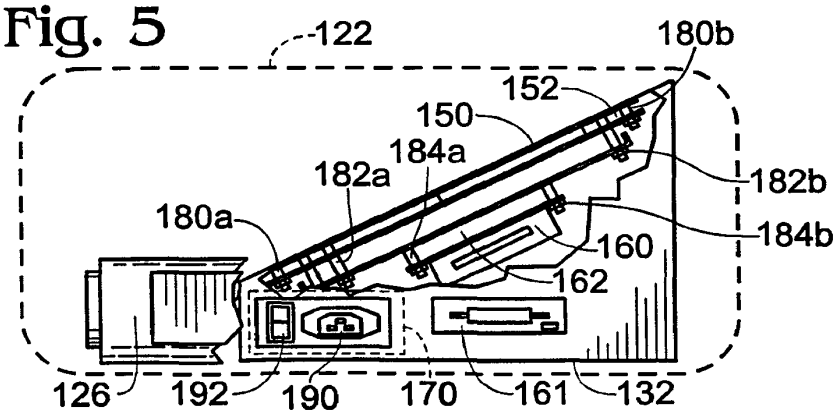


Fig. 8

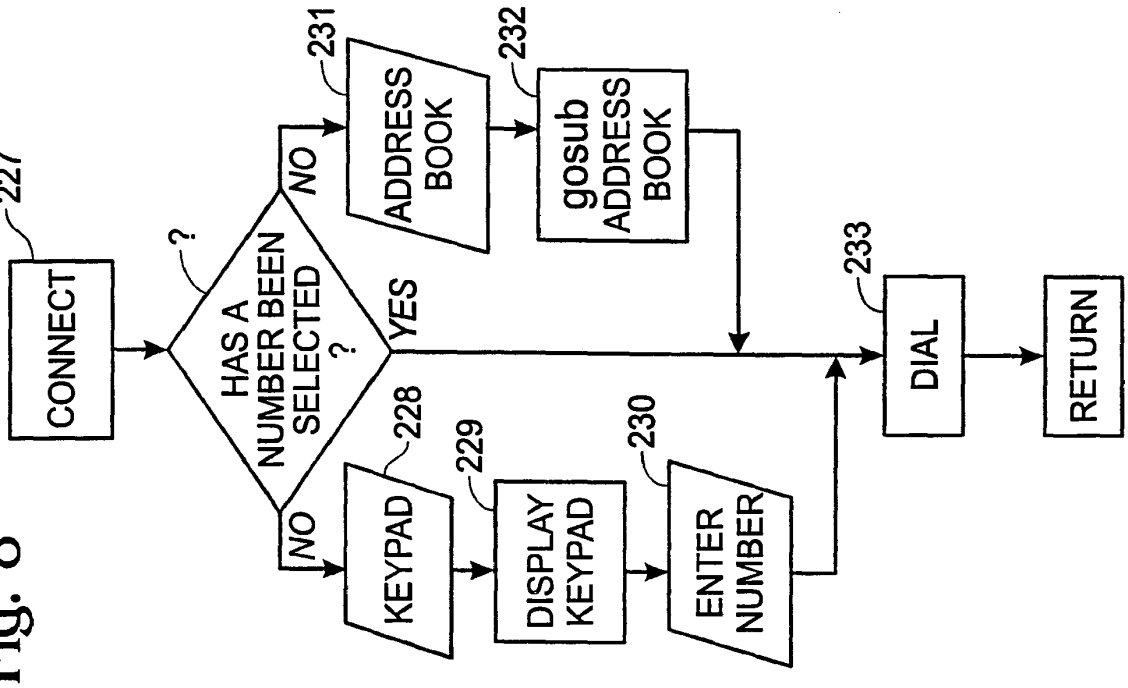

227
CONNECT
HAS A NUMBER BEEN SELECTED ?
YES
NO
231
ADDRESS BOOK
232
gosub ADDRESS BOOK
228
KEYPAD
229
DISPLAY KEYPAD
230
ENTER NUMBER
233
DIAL
RETURN

Fig. 7

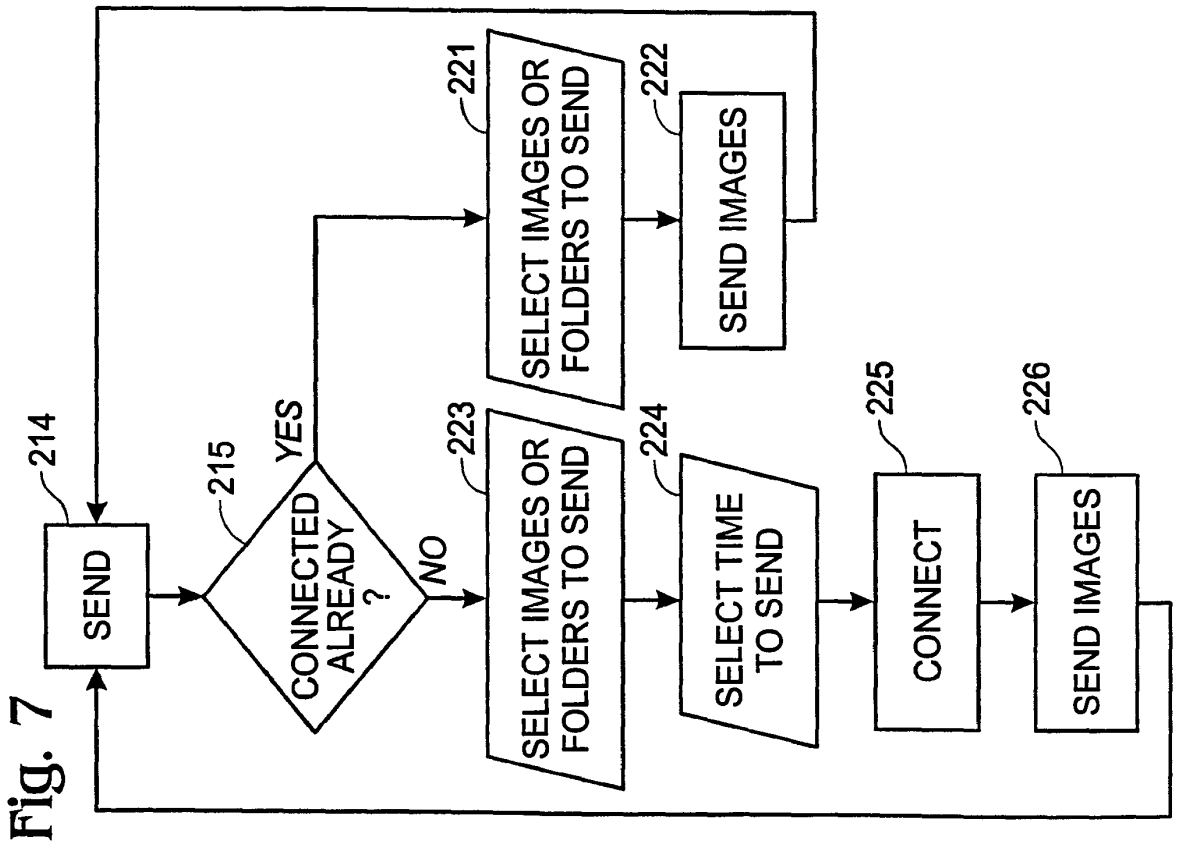

214
SEND
215
CONNECTED ALREADY ?
YES
NO
221
SELECT IMAGES OR FOLDERS TO SEND
222
SEND IMAGES
223
SELECT IMAGES OR FOLDERS TO SEND
224
SELECT TIME TO SEND
225
CONNECT
226
SEND IMAGES

Fig. 9

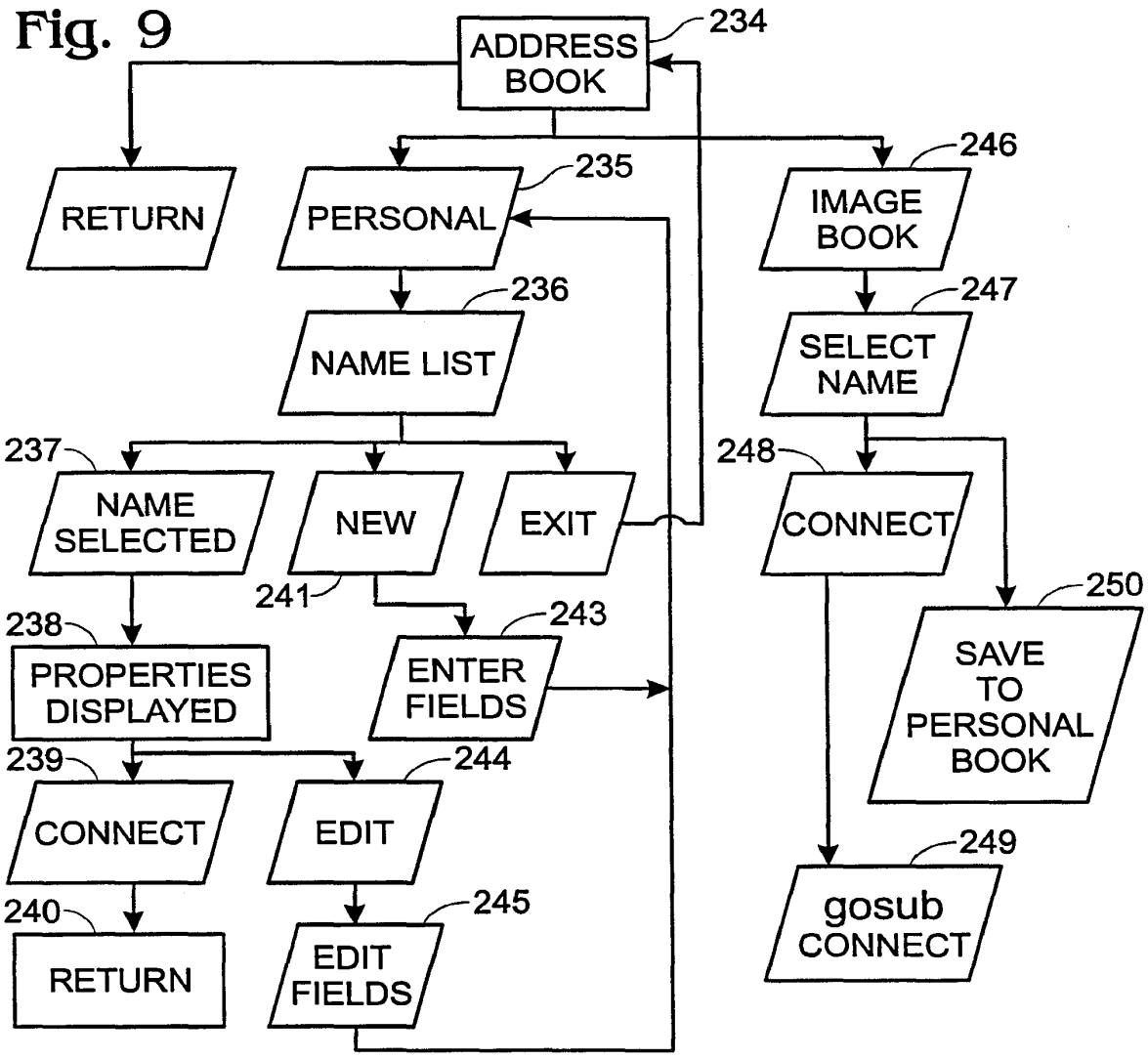

ADDRESS BOOK
234
RETURN
PERSONAL
235
IMAGE BOOK
246
NAME LIST
236
SELECT NAME
247
NAME SELECTED
237
NEW
EXIT
CONNECT
248
241
ENTER FIELDS
243
SAVE TO PERSONAL BOOK
250
PROPERTIES DISPLAYED
238
CONNECT
239
EDIT
244
gosub CONNECT
249
RETURN
240
EDIT FIELDS
245

Fig. 14

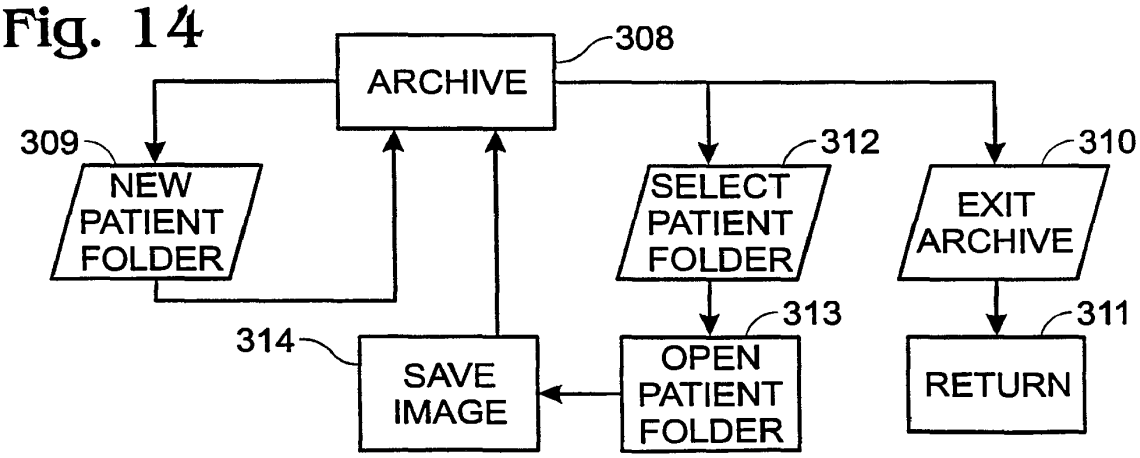

ARCHIVE
308
NEW PATIENT FOLDER
309
SELECT PATIENT FOLDER
312
EXIT ARCHIVE
310
SAVE IMAGE
314
OPEN PATIENT FOLDER
313
RETURN
311

Fig. 10

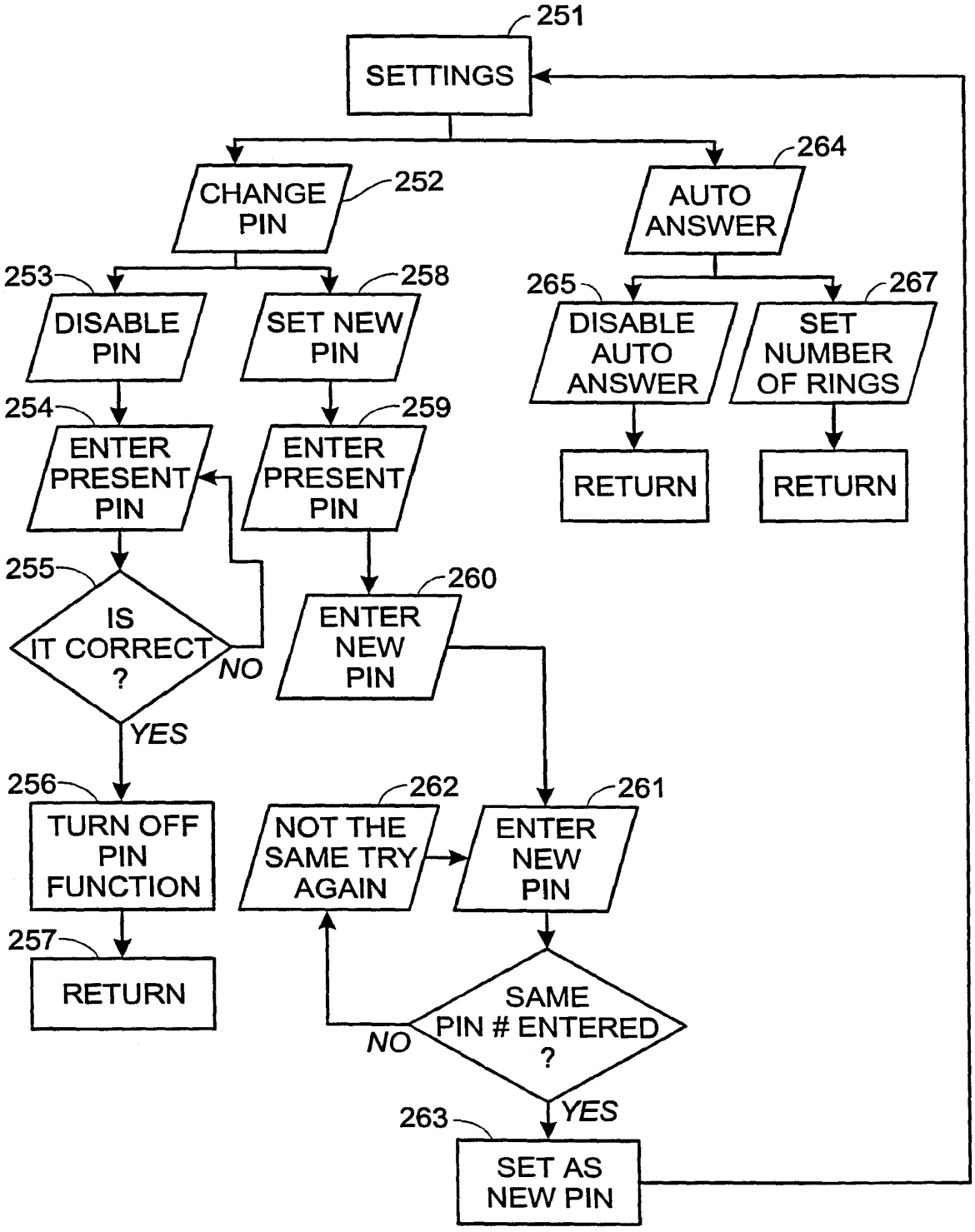

251
SETTINGS
CHANGE PIN
252
AUTO ANSWER
264
253
DISABLE PIN
258
SET NEW PIN
265
DISABLE AUTO ANSWER
267
SET NUMBER OF RINGS
254
ENTER PRESENT PIN
259
ENTER PRESENT PIN
RETURN
RETURN
255
IS IT CORRECT ?
NO
260
ENTER NEW PIN
YES
256
TURN OFF PIN FUNCTION
262
NOT THE SAME TRY AGAIN
261
ENTER NEW PIN
257
RETURN
SAME PIN # ENTERED ?
NO
YES
263
SET AS NEW PIN

Fig. 11

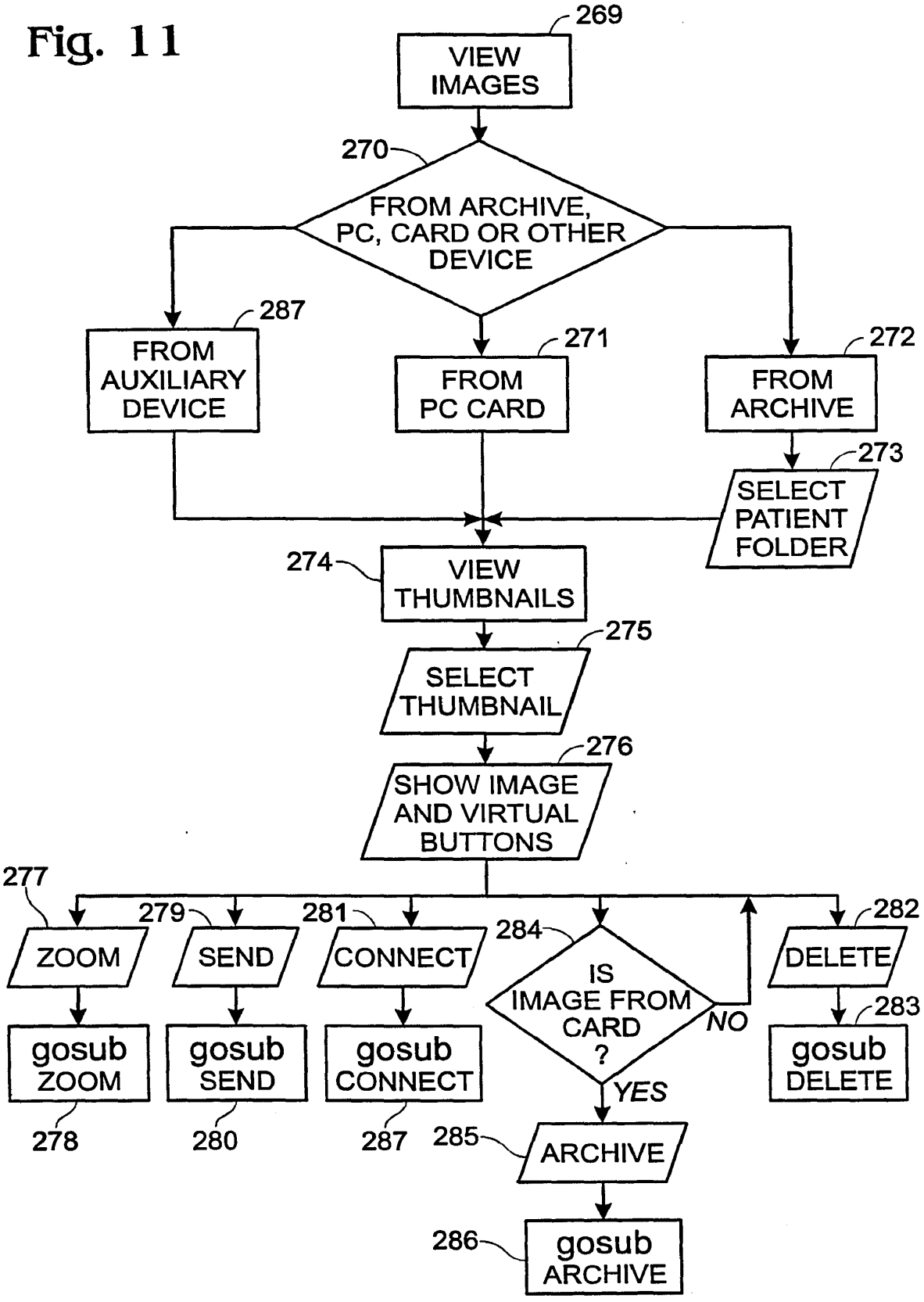

269
VIEW IMAGES
270
FROM ARCHIVE, PC, CARD OR OTHER DEVICE
287
FROM AUXILIARY DEVICE
271
FROM PC CARD
272
FROM ARCHIVE
273
SELECT PATIENT FOLDER
274
VIEW THUMBNAILS
275
SELECT THUMBNAIL
276
SHOW IMAGE AND VIRTUAL BUTTONS
277
ZOOM
279
SEND
281
CONNECT
284
IS IMAGE FROM CARD ?
NO
YES
282
DELETE
283
gosub DELETE
gosub ZOOM
278
gosub SEND
280
gosub CONNECT
287
285
ARCHIVE
286
gosub ARCHIVE

Fig. 12

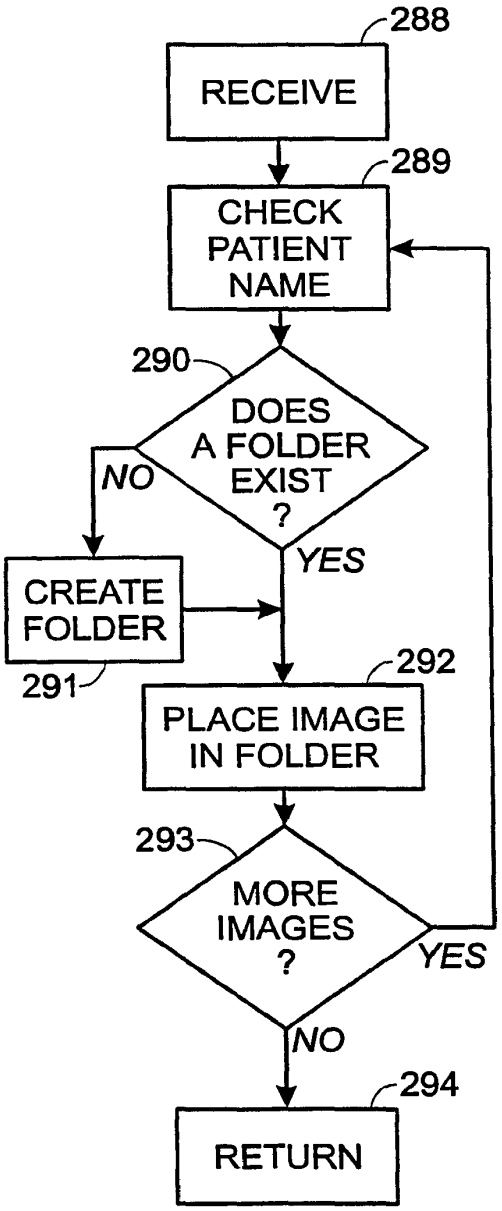

288
RECEIVE
289
CHECK PATIENT NAME
290
DOES A FOLDER EXIST ?
NO
YES
CREATE FOLDER
291
292
PLACE IMAGE IN FOLDER
293
MORE IMAGES ?
YES
NO
294
RETURN

Fig. 16

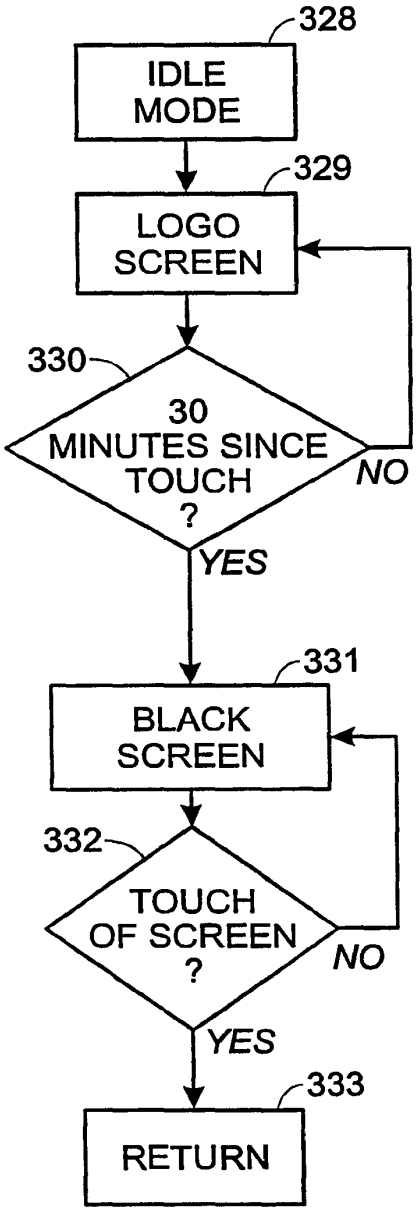
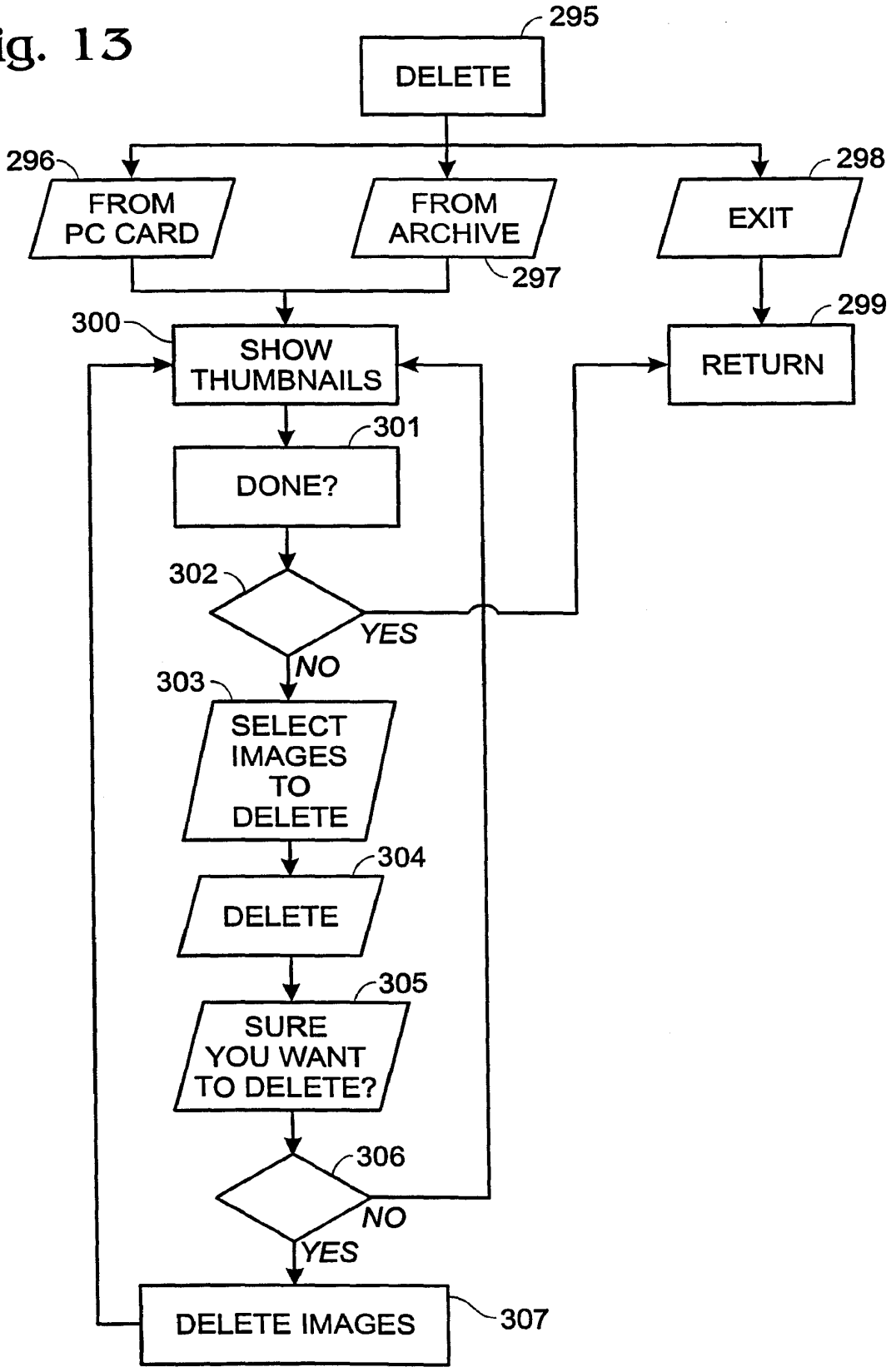

328
IDLE MODE
329
LOGO SCREEN
330
30 MINUTES SINCE TOUCH ?
NO
YES
331
BLACK SCREEN
332
TOUCH OF SCREEN ?
NO
YES
333
RETURN

Fig. 13


295
DELETE
296
FROM PC CARD
FROM ARCHIVE
297
298
EXIT
299
RETURN
300
SHOW THUMBNAILS
301
DONE?
302
YES
NO
303
SELECT IMAGES TO DELETE
304
DELETE
305
SURE YOU WANT TO DELETE?
306
NO
YES
DELETE IMAGES
307

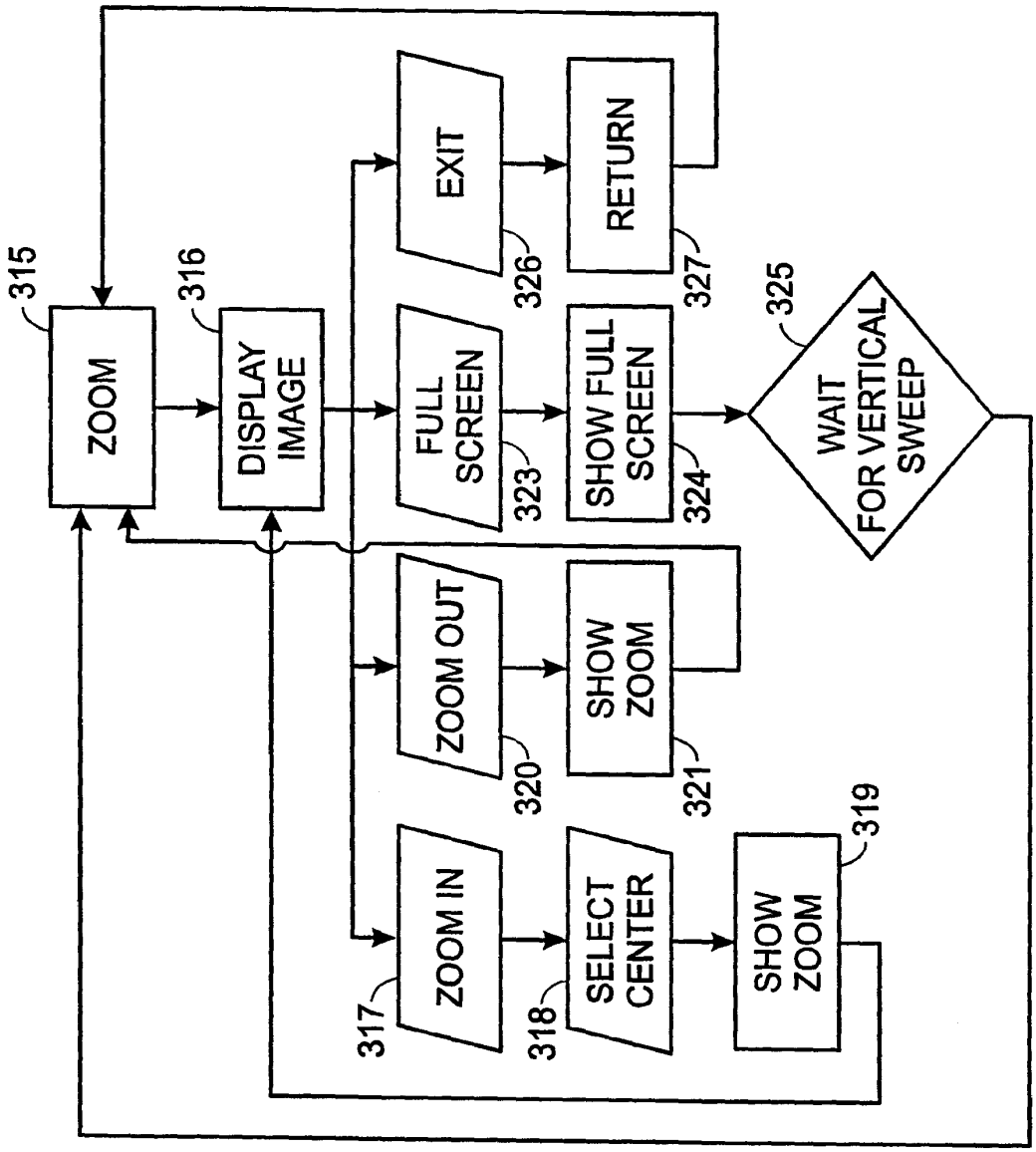

ZOOM
315
DISPLAY IMAGE
316
FULL SCREEN
323
SHOW FULL SCREEN
324
EXIT
326
RETURN
327
WAIT FOR VERTICAL SWEEP
325
ZOOM OUT
320
SHOW ZOOM
321
ZOOM IN
317
SELECT CENTER
318
SHOW ZOOM
319

Fig. 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/13566

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G09G 5/00
US CL :345/2, 127, 901
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 345/1, 2, 115, 116, 121, 127, 131, 169, 329, 342, 348, 901.

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,634,018 A (TANIKOSHI ET AL) 27 MAY 1997, COL. 7, LINES 33-67 AND COL. 9, LINES 1-50.	1-2, 5, 7-8, 11, 16-17 --- 3-4,6,9-10, 12-15, 18-20
Y	US 5,544,300 A (SKARBO ET AL) 06 AUGUST 1996, COL. 7, LINES 25-51 AND COL. 9, LINES 1-14.	3, 4, 6
Y	US 5,508,713 A (OKOUCHI) 16 APRIL 1996, COL. 6, LINES 48-54 AND COL. 10, LINES 23-29.	9-10, 12-15, 18-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 04 OCTOBER 1998	Date of mailing of the international search report 17 NOV 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer CHANH NGUYEN Telephone No. (703) 305-6603

Form PCT/ISA/210 (second sheet)(July 1992)★

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 September 2001 (13.09.2001)

PCT

(10) International Publication Number
WO 01/67707 A2

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/US01/06707

(22) International Filing Date: 2 March 2001 (02.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/186,693	3 March 2000 (03.03.2000)	US
60/186,774	3 March 2000 (03.03.2000)	US
09/695,499	23 October 2000 (23.10.2000)	US
09/753,141	29 December 2000 (29.12.2000)	US

(71) Applicant *(for all designated States except US)*: **SCALE EIGHT, INC.** [US/US]; 625 Second Street, Suite 201, San Francisco, CA 94107 (US).

(72) Inventors; and

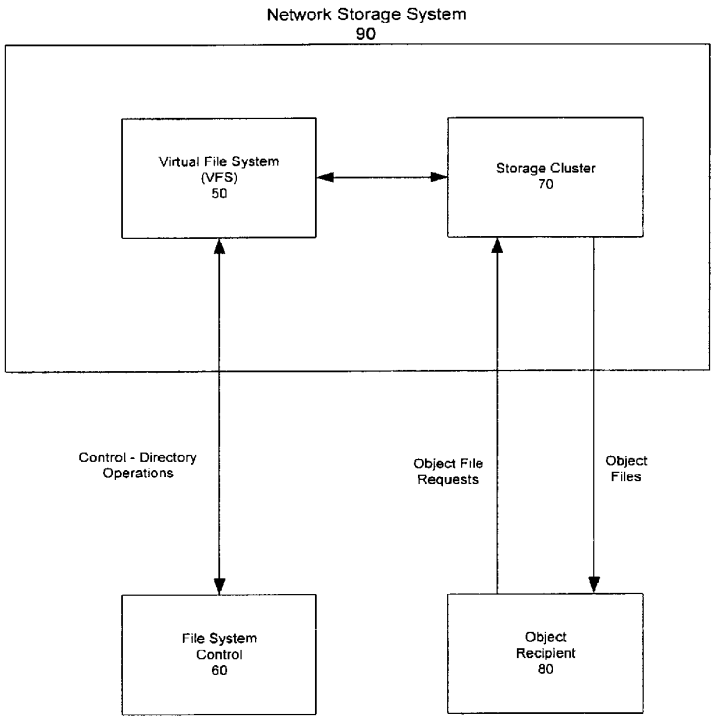
(75) Inventors/Applicants *(for US only)*: **COATES, Joshua, L.** [US/US]; 70 Brookwood Road, Orinda, CA 94563 (US). **JONES, F., Alan** [US/US]; 415 Pope Street, Menlo Park, CA 94025 (US). **RUSSEL, Georgina, L.** [US/US]; 899 Oak Street #4, San Francisco, CA 94117 (US). **GONZALEZ, Michael** [US/US]; 20949 Wilbeam Avenue, Castro Valley, CA 94546 (US). **BOZEMAN, Patrick, E.** [—/US]; 500 Beale Street #311, San Francisco, CA 94105 (US). **GAUTIER, Taylor** [US/US]; 708 38th Avenue #3, San Francisco, CA 94121 (US). **PATTERSON, David, A.** [US/US]; 114 Purdue Avenue, Kensington, CA 94708 (US).

(74) Agent: **STATTLER, John**; Stattler Johansen & Adeli LLP, P.O. Box 51860, Palo Alto, CA 94303-0728 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,

[Continued on next page]

(54) Title: A NETWORK STORAGE SYSTEM



(57) Abstract: A network storage system includes a virtual file system ("VFS"), to manage the files of the network storage system, and a storage center that stores the files. The VFS and the storage center are separated, such that a client accesses the VFS to conduct file system operations and the client accesses the storage center to upload/download files. The client accesses the network storage system through one or more storage ports. The storage center includes a plurality of distributed object storage managers (DOSMs) and a storage cluster that includes a plurality of intelligent storage nodes. The network storage system includes additional storage centers at geographically disparate locations. The network storage system uses a multi-cast protocol to maintain file information at the DOSMs regarding files stored in the intelligent storage nodes, including files stored in disparate storage centers.

WO 01/67707 A2

CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A NETWORK STORAGE SYSTEM

BACKGROUND OF THE INVENTION

Field of the Invention:

The present invention is directed toward the field of storage, and more particularly toward accessing remote storage through use of a local device.

Art Background:

With the rapid digitization of music, film and photographs, customer demand is driving the Internet to become the most preferred transport mechanism for all forms of digital media. Using the Internet, users have instantaneous worldwide access to their favorite movies, songs, or personal memorabilia. As the producers and owners of media content increasingly use the Internet as a primary method for worldwide distribution, the aggregate amount of rich media content available over the Internet is increasing at an extremely rapid rate.

Not only is the number of rich media objects available over the Internet growing exponentially, but the size of the media, generally referred to herein as objects, is also dramatically increasing. A median Web object is 5 kilobytes (KB) in size, while the size of a rich media object may be 100 to 1 million times larger. For example, high-resolution digital photographs average 500 KB per picture. Digital music runs 3 to 5 megabytes ("MB") per song, and digital movies may reach up to 4 gigabytes ("GB") in size.

As the number of personal computers, digital camcorders, digital cameras, and personal digital audio players grow, demand for Internet bandwidth to store, share and retrieve media files across the Internet also will grow. As the use of high-bandwidth digital subscriber lines ("DSL"), cable modems, and digital broadcast satellite networks gain in popularity, which supports the growth of the Internet backbone, the demand for using the Internet as a primary delivery channel for rich media objects also gains in popularity. This development causes a virtuous cycle, where the installation of broadband networks drives the use of rich media devices, which in turn, creates demand for further improvements in network bandwidth, and so on.

The distribution of rich media objects across the Internet creates the need for increased storage capacity to store these rich media objects. As the number of personal

media devices grows, and the network bandwidth expands, the amount of storage media required to store the various MP3 files, photographs, films, and video clips will also grow. Also, as more storage becomes readily available, more people will use the Internet to catalog, store, and access their rich media objects (*e.g.*, digital photographs of family members).

To date, only traditional storage solutions from established enterprise vendors have been available to a Web site developer implementing rich media repositories. One challenge with adopting today's existing storage technology for use with the Internet is meeting current and future scalability requirements. Today, large scale storage systems only scale to a few dozen terabytes. This amount of storage space is inadequate for storing substantial amounts of rich media objects. For example, if just 10 percent of America on line ("AOL") users place two 15 minute videos on a personal home page, then one petabyte (*i.e.*, 1000 terabytes) of storage would be required. Today's enterprise storage system architectures cannot support this level of storage capacity.

In the Internet world, in addition to providing mass storage, it is also critically important to provide universal access to that storage across the wide area network. The content provider, regardless of the location of their content servers, cache servers, or stream servers, would ideally like to provide ubiquitous access to an entire store of rich media objects. Current technology, including storage area networks and network attached storage technologies, do not provide direct access to the wide area network. Only servers located within the same metropolitan area can directly access these types of storage systems.

Since Internet users are measured in the tens of thousands or even millions of users, instead of hundreds of users, another challenge in mass storage is the ability to scale delivery of media as the demand increases. A true Internet based storage system must be able to handle peak loads of millions of simultaneous requests from all around the world. Traditional storage architectures are designed to support a few hundred simultaneous requests from the fastest possible response time to match the speed of the server CPU. For the Internet, storage systems must be able to manage literally millions of simultaneous downloads at the speed of the wide area network. Thus, these traditional storage architectures are not "impedance matched" with the wide area network because the storage devices handle far too few simultaneous transactions that far exceed the latency requirements of the wide area network. In addition, these traditional storage architectures are typically implemented with expensive disks and expensive connection technologies.

Another issue regarding storage of rich media objects is the time to market. The time to market is often a crucial requirement for new rich media Web sites. Growth rates are measured in terabytes per month. Quickly bringing new capacity online becomes a strategic advantage in fast-moving markets. Typically, with traditional storage solutions, it takes a customer two to six months to integrate a fully operational multi-terabytes storage unit with the content providers site. This start-up time is to slow to meet rapidly increasing business demands. Pre-building large amounts of excess capacity in anticipation of this demand is one tactic to deal with unpredictable demand spikes, but this approach is prohibitively expensive.

Traditional storage architectures have been optimized for database and file server applications. The Internet introduces a whole new set of demands on storage devices, including scalability, global access, user accounts, and rapid deployment. With the explosive growth in rich media served over the Internet over the next several years, this is coming to a head. The coming title wave of rich content will surpass the capabilities of even the most robust enterprise storage architectures. Accordingly, there is a demand to develop new paradigms in new ways of designing Internet ready rich media storage systems.

SUMMARY OF THE INVENTION

A network storage system includes a virtual file system ("VFS") and a storage center. The VFS stores file system information to manage the files of the network storage system. The storage center stores the files of the network storage system. The VFS and the storage center are separated, such that a client accesses the VFS to conduct file system operations and the client accesses the storage center to upload/download files.

In one embodiment, the client accesses the network storage system (*e.g.*, virtual file system and the storage center) through a storage port. The storage port provides access to a client's files of the network storage system. In one embodiment, the client mounts the storage port, through a standard NFS or CIFS operation, and performs file system operations and accesses by issuing local file system operations to the storage port. In response, the storage port translates the local file system operations to network storage system operations. Additional storage ports may be configured at the client to access the network storage system in the event of a failover condition.

In one embodiment, the storage center includes a plurality of distributed object storage managers (DOSMs) and a storage cluster that includes a plurality of intelligent

storage nodes. The DOSMs receive requests to access the storage center. The intelligent storage nodes store the files of the network storage system and service access requests from the DOSMs. The network storage system includes additional storage centers at geographically disparate locations. In one embodiment, the network storage system uses a multi-cast protocol to maintain file information at the DOSMs regarding files stored in the intelligent storage nodes, including files stored in disparate storage centers. The storage center further includes a load balancing fabric. The load balancing fabric selects a DOSM for an access request based on demand to access the storage center. In addition, the DOSMs include a data cache for caching at least a subset of files stored in the intelligent storage nodes. The use of load balancing in the storage center results in caching data for files in high demand in the data caches of the DOSMs.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating one embodiment for the storage system of the present invention.

Figure 2 illustrates one embodiment for use of the network storage system as a media storage service.

Figure 3 is a block diagram illustrating one embodiment for the storage cluster.

Figure 4 is a flow diagram illustrating one embodiment for the download operation in the storage cluster.

Figure 5 is a flowchart illustrating one embodiment for authentication in the network storage system.

Figure 6 illustrates one embodiment of a distributed object storage manager ("DOSM").

Figure 7 is a block diagram illustrating one embodiment for an intelligent storage node.

Figure 8 is a flow diagram illustrating one embodiment for processing upload requests in the storage cluster.

Figure 9 is a flow diagram illustrating one embodiment for generating unique fingerprints of object files.

Figure 10 is a block diagram illustrating one embodiment for caching data in the storage cluster.

Figure 11 is a block diagram illustrating one embodiment for implementing a VFS for use with a network storage system.

Figure 12 illustrates example database tables for implementing the file system with a database.

Figures 13A and 13B are flow diagrams illustrating one embodiment for performing directory operations in the VFS.

Figure 14 is a flow diagram illustrating one embodiment for the delete file operation for the network storage system.

Figure 15 illustrates geographical replications of storage centers.

Figure 16 is a block diagram illustrating one embodiment for replicating the storage centers.

Figure 17 illustrates one embodiment for use of the storage center in a content delivery network.

Figure 18 is a flow diagram illustrating one embodiment for use of the storage center with a content delivery network.

Figure 19 illustrates one embodiment for use of the storage port in the network storage system.

Figure 20 is a flow diagram illustrating one embodiment for use of a storage port to deliver content.

Figure 21a illustrates one hardware configuration for a storage port device.

Figure 21b illustrates embodiments for implementing the storage port in software.

Figure 22 is a block diagram illustrating one embodiment for a storage port.

Figure 23 is a block diagram illustrating one embodiment for file system translation in the storage port.

Figure 24 is a flow diagram illustrating one embodiment for translating a file system operation from a local file system to the network storage file system.

Figure 25 is a block diagram illustrating one embodiment for using the storage port to directly download object files to the end-user.

Figure 26 is a flow diagram illustrating one embodiment for directly downloading object files to an end-user.

Figure 27 is a block diagram illustrating one embodiment to interface a storage center to a client's private file directory system.

Figure 28 is a flow diagram illustrating one embodiment for accessing object files in a storage center using a client's private file system.

Figure 29 is a block diagram illustrating one embodiment for a storage port fail over configuration.

Figure 30 is a flow diagram illustrating one embodiment for a storage port fail over process.

Figure 31 is a flow diagram illustrating one embodiment for using the multicast protocol after a storage node fail over condition.

DETAILED DESCRIPTION

Network Storage System Overview:

The network storage system is designed to meet the storage requirements of rich media content owners. Rich media objects typically represent up to 90 percent of the storage required for a film, music or a photo album associated with a web site. The network storage system uses distributed systems technology to provide scalability to support petabytes of storage and to support millions of users. Users only gain access to their media objects, within the network storage system, using a highly secured "shared secret" authentication certificate technology. The network storage system also provides immediate expandability for any user that desires to increase their storage capacity. Also, the network storage system is extremely cost-effective because, in one embodiment, it consists of standard off the shelf CPUs with the latest high-density disk technology.

For purposes of nomenclature, the term "client", as used herein, refers to an entity that uses the storage system to store object files. For example, a client may consist of a web site owner that desires to deliver, outside their web server, rich media objects associated with content on their web site. Also, for purposes of nomenclature, the term "end-user", as used herein, refers to a recipient of the object. For example, the end-user may consist of a computer user that downloads objects from a web site across the Internet using a web browser. Also, under this definition, the end-user may also be a client.

Figure 1 is a block diagram illustrating one embodiment for the storage system of the present invention. For the embodiment of Figure 1, the storage system consists of a control path and a data path. The control path consists of a virtual file system ("VFS") 50 and the data path consists of a distributed storage cluster 70. The control path is used to conduct all

directory operations. The VFS includes, in part, client assigned filenames and network storage system assigned unique file identifiers for each rich media object. The unique file identifiers are embedded into storage resource locators ("SRLs").

The distributed storage cluster 70 is used to store the object files for the system (*i.e.*, all client data). As shown in Figure 1, the VFS and the storage cluster 70 are coupled to communicate information so as to coordinate file system information with the physical storage of the object files.

As shown in Figure 1, file system control 60 issues directory operation requests to the VFS 50. As is described more fully below, file system control 60 may comprise software that uses a library to essentially "translate" file system requests from the client's local file system to file system requests compatible with the network storage system. In other embodiments, file system control 60 consists of a storage port coupled to the client's system (*e.g.*, the client's application or web server). In general, the storage port, implemented in either hardware or software, translates file system commands from the client's local file system (*e.g.*, NFS or CIFS) to file system requests compatible with the network storage system. In one embodiment, to interface the client's file system to the network storage system, a client need only mount the storage port as a network drive. The storage port then provides complete access to the network storage system. A detailed discussion of the storage port is set forth below.

As shown in Figure 1, object recipient 80 receives, in response to object requests, objects downloaded from storage cluster 70. The object recipient 80 may comprise the client, or the object recipient 80 may consist of one or more end-users. Embodiments for transferring objects from the storage cluster 70 to object recipients, including both end-users and clients, are described more fully below.

The network storage system has applications for use as an Internet based media storage service. For this application, the network storage system is an integral part of the Internet infrastructure used by rich media content owners and delivery networks. Figure 2 illustrates one embodiment for use of the network storage system as a media storage service. In general, the storage service 130 provides a single consistent worldwide image of a client's (*e.g.*, a company operating a web site) entire directory of rich objects. For this embodiment, an end-user 100 is coupled to both the content origin server 120 and storage service 130 through a network. For example, the end-user 100 may be coupled to the content origin server 120 and storage service 130 via the Internet. The storage service 130 includes

processing and networking facilities, such as a server 140, and data store 150. The storage service 130 and content origin server 120 communicate to conduct file directory operations and object file operations. The data store 150, part of the storage service 130, stores large data files, such as rich media data files, illustrated as multimedia files 160, 170 and 180 in Figure 2. In one embodiment, the data store 150 consists of a cluster of intelligent storage nodes.

In one embodiment, the storage service communicates with web servers (*e.g.*, content origin server 120) and browsers (*e.g.*, Microsoft Explorer or Netscape Navigator) operating on end-user computer 100 via the standard Internet hypertext transfer protocol ("HTTP") and universal resource locators ("URLs"). Although the use of HTTP is described herein, any transport protocol may be used without deviating from the spirit or scope of the invention. For the configuration of Figure 2, the end-user, through end-user computer 100, generates hyper text transfer protocol ("HTTP") requests to the content origin server 120 to obtain hyper text mark-up language ("HTML") files. In addition, to obtain large data objects associated with those text files, the end-user, through end user computer 100, generates HTTP requests to the storage service 130. For example, the end-user may download from the content origins server 120 a few kilobytes of textual data describing a rich object, such as text describing an upcoming film. When the user "clicks" on a URL to download a film snippet from the upcoming film, an HTTP request is generated to the storage service 130, and a storage service 130 downloads the film snippet to the end-user computer 100. The network configuration of Figure 2 permits off loading the storage of rich objects from the content origin server 120 to the storage service 130. This configuration greatly reduces the size and complexity of content origin servers needed to store, manage and serve rich objects to end-users.

Distributed Storage Cluster:

In one embodiment, the storage cluster utilizes distributed systems technology that harnesses the throughput of hundreds of CPUs and the storage of thousands of disk drives. Figure 3 is a block diagram illustrating one embodiment for the storage cluster. The storage cluster 300 receives upload, download, and delete operations that include the storage resource locator ("SRL"). The SRL is then used to uniquely identify a client file. As shown in Figure 3, the storage cluster consists of distributed object storage managers ("DOSMs") 320 and intelligent storage nodes 340. There are "n" distributed object storage managers 320,

wherein "n" is any integer value greater than one. Similarly, there are "n" intelligent storage nodes for the intelligent storage nodes 340 component (*i.e.*, wherein "n" is also any integer value greater than one).

As shown in Figure 3, file upload and download operations are input to a load balancing fabric 310. In one embodiment, the load balancing fabric 310 is a layer four ("L4") switch. In general, L4 switches are capable of effectively prioritizing TCP and UDP traffic. In addition, L4 switches, which incorporate load balancing capabilities, distribute requests for HTTP sessions among a number of resources, such as servers. For this embodiment, the load balancing fabric 310 distributes upload and download requests to one of a plurality of DOSMs based on DOSM availability. The load balancing capability in an L4 switch is currently commercially available.

Each DOSM independently handles hundreds of simultaneous download transactions. In one embodiment described below, each DOSM has a local high-speed disk cache to store frequently accessed file objects. Each DOSM has a map, dynamically generated, of the storage system. The map identifies a correspondence between an intelligent storage node address and an object finger print. In one embodiment, the DOSMs record all usage and performance data gathered by a separate accounting system and monitoring system.

The DOSMs 320 communicate with the intelligent storage nodes 340 via an interconnect fabric 330. The interconnect fabric 330 consists of a high-speed, high bandwidth fabric to ensure that all the DOSMs 320 communicate with every intelligent storage node at all times. In one embodiment, the DOSMs 320 communicate with the intelligent storage node over the interconnect fabric via a protocol, entitled the distributed object storage protocol ("DOSP"). Effectively, the DOSP links hundreds of intelligent storage nodes into one large storage cluster. As described more fully below, the DOSP consist of a multi-cast protocol as well as a point-to-point protocol.

In general, the intelligent storage nodes 340 provide the persistent store for the objects or files. The intelligent storage nodes contain thousands of high-density disk drives. The intelligent storage nodes are described more fully below in conjunction with the discussion of Figure 7.

In one embodiment, the network storage system uses the storage resource locators ("SRLs") to process requests. In one embodiment, the network storage system uses the following format for the SRL:

http://<storage-cluster>/<encoded-request>/<digital-signature>/<arbitrary-customer-uri,

wherein:

the "storage-cluster" field includes the name or IP address of a storage center DSM pool;

the "encoded-request" field comprises a base64 encoded op code and arguments;

the "digital-signature" field consists of a certificate derived from the following expression: md5(shared-secret + md5(shared-secret + encoded-request)); and

the "arbitrary-customer-uri" field contains arbitrary information added to the SRL by the network storage system clients. For example, the arbitrary-customer-uri field may include the filename and extension of the file being downloaded to enable browsers to send the content to an appropriate plug-in.

In one embodiment, the "encoded request" field is encoded using base64 encoding. As shown in Table 1, the encoded request consists of a URL type field, a version field, and type/version specific payload field.

Table 1

Field	Datatype	Comment
Type	Numeric	Type of the URL, i.e. Standard, CDN, etc.
Version	Numeric	Version of the URL
Payload	NA	Payload specific to the Type/Version of the URL.

In one embodiment, the type/version specific payload field consists of a series of '/' delimited fields that contain accounting information, an op code, and an op code dependent argument list. Table 2 shows one embodiment for the type/version specific payload field.

Table 2

Field	Datatype	Comment
Expires	Numeric	Number of seconds since the epoc that the link expires. If 0, the link has an infinite duration and will not be checked for expiration.
Access method	Numeric	The access method associated with the SRL, i.e. Storage Port, end user SRL, CDN, etc.
Client Id	Numeric	The client id of the client performing the operation.
Op Code	Numeric	The opcode of the operation to be performed.
Arguments	NA	An opcode specific argument list.

Table 3 includes two access method types for the access method field.

Table 3

Access method	Encoding	Comment
8RL	0x0001	End user SRL request.
MediaPort	0x0002	Internal Storage Port request.

Table 4 includes operational codes for the op code field.

Table 4

Operation	Encoding	Arguments
NO_OP	0x0000	None
STORE	0x0010	Pfid – numeric Parent folder id to upload the file to. Other arguments are mime encoded.
FETCH	0x0020	Md5 – alphanumeric Hexadecimal representation of the md5 hash of the file to be downloaded.
FETCH_AUTH	0x0021	Md5 – alphanumeric Hexadecimal representation of the md5 hash of the file to be downloaded. Authentication Callback URI – alphanumeric URL encoded callback URI
DELETE	0x0050	Md5 – alphanumeric Hexadecimal representation of the md5 hash of the file to be deleted.
CONTROL	0x1000	ControlTicket – alphanumeric Hexadecimal representation of the digital signature of the XML control document.

Figure 4 is a flow diagram illustrating one embodiment for the download operation in the storage cluster. For purposes of nomenclature, the "recipient" in a download operation is the destination of the file for the download operation. The storage cluster receives a download request, including the unique file identifier (*e.g.*, SRL) (block 400, Figure 4). When the storage cluster receives a download request, the load balancing fabric 310 (Figure 3), such as an L4 switch, selects an available DOSM (block 410, Figure 4). The DOSM parses the SRL to extract the certificate and the encoded request (block 415, Figure 4). From the encoded request, a certificate is calculated, and the calculated certificate is compared to the SRL certificate. If the SRL does not authenticate, then an error message is sent to the recipient (blocks 420 and 425, Figure 4). Alternatively, if the SRL does

authenticate, then the DOSM determines whether the object identified by the SRL resides in the corresponding DOSM's data cache (blocks 420 and 430, Figure 4). If the data object is cached, then the object is transmitted from the storage cluster to the recipient (*e.g.*, via the Internet using HTTP protocol) (blocks 430 and 495, Figure 4). If the object is not cached at the DOSM, then the DOSM attempts to identify the location of the object in one of the intelligent storage nodes (blocks 430 and 440, Figure 4).

If the DOSM knows the location of the object (*e.g.*, the object file is an entry in the DOSM look-up table) and the storage node is readable, then the DOSM obtains a connection with the storage node that stores the object, and transmits the object from the storage cluster to the recipient (blocks 442, 435 and 495, Figure 4). Alternatively, if the DOSM does not know the storage location of the object in the intelligent storage nodes, then the DOSM broadcasts a request to the intelligent storage nodes to locate the object (blocks 440 and 450, Figure 4). Each intelligent storage node determines whether the object is stored on one of its disk drives (block 460, Figure 4). If the object file is located in one of the intelligent storage nodes, then the intelligent storage node, which stores the requested object, broadcasts identification information to all of the distributed object storage managers (blocks 462 and 470, Figure 4). For example, if intelligent storage node "1" of intelligent storage nodes 340 stores the requested object in disk "3", then intelligent storage node "1" broadcasts to all "n" DOSMs that the object file is located in disk "3" of intelligent storage node"1." All DOSMs snoop on the bus to obtain file identification information. In response to the intelligent storage nodes broadcast, each DOSM updates its lookup table or file system directory with the proper file identification information.

If the DOSM broadcasts a request to the intelligent storage nodes to locate the object and the object is not located from the request, then the DOSM establishes a point-to-point connection with an intelligent storage node to individually query the storage node for the object (blocks 462 and 464, Figure 4). This process is repeated until all intelligent storage nodes have been queried or the object has been located. If the object is located in one of the intelligent storage nodes, then the intelligent storage node, which stores the requested object, broadcasts identification information to all of the distributed object storage managers (blocks 466 and 470, Figure 4). Alternatively, if the object is not located in one of the intelligent storage nodes, then a failover procedure is executed to locate the object in a different storage center (blocks 466 and 468, Figure 4).

When the intelligent storage node is located, the DOSM obtains a connection with th intelligent storage node, and opens the file with the requested object. If the storage node i readable (*i.e.*, the DOSM successfully reads the file from the storage node), then the object i transmitted from the intelligent storage node to the recipient via a network (*e.g.*, using HTT protocol over the Internet). If the object file is not readable, then a failover procedure i executed to obtain the object in a different storage node and/or storage center, and the DOSM obtains a connection with the new storage node (blocks 442, 468 and 435, Figure 4) Thereafter, the object is transmitted from the storage cluster to the recipient (block 49 Figure 4).

In one embodiment, accesses to the network storage system require a vali authentication certificate. In one embodiment utilizing CDNs, the certificate is based on th object file's unique user filename and a secure key assigned to each client account. In othe embodiments, the network storage system supports full HTTPS and SSL protocols for secur communications between clients/end-users and the network storage system.

Figure 5 is a flowchart illustrating one embodiment for authentication in the networ storage system. To authenticate a request, the network storage system decodes the SRL t extract the client identification, the SRL certificate and the client filename or objec fingerprint (block 500, Figure 5). The network storage system (*i.e.*, virtual file system o storage cluster) extracts a "secret" or secure key corresponding to the client identified wit the request. In general, the "secret" or secure key is a password supplied by the client t authenticate operations in the network storage system. Using the secure key and objec fingerprint, the network storage system generates a calculated certificate (block 52(Figure 5). In one embodiment, the network storage system generates a calculated certificat for the request in accordance with the following expression:

MD5 Hash (Secure Key + *MD5 Hash* (Secure Key + Encoded SRL))

As shown above, a first MD5 hash calculation is performed on the object fingerprin and the secure key to obtain a first result, and a second MD5 hash calculation is performed o the first result and the secure key to obtain the calculated certificate. The network storag system compares the calculated certificate with the SRL certificate (*i.e.*, the certificat transmitted with the SRL request) (block 530, Figure 5). If the certificates match, then th SRL is authenticated, and the request is performed (blocks 540 and 560, Figure 5) Alternatively, if the calculated certificate does not match the SRL certificate, then th

network storage system generates an error message to the requester (blocks 540 and 550, Figure 5).

Figure 6 illustrates one embodiment of a distributed object storage manager ("DOSM"). For this embodiment, the processes and functions of each DOSM are implemented in software for execution on a computer, such as a server 600. In other embodiments, the distributed object storage managers 320 may be implemented in a combination of hardware and software on one or more computers. Each DOSM maintains a file lookup table to identify the location of object files stored in the intelligent storage nodes 340. Table 610 of Figure 6 illustrates one embodiment for a DOSM file lookup table. For this embodiment, each entry of the table identifies a corresponding object file stored in an intelligent storage node. Specifically, each entry includes a file identification, an IP address, and a disk identification. The file identification, also referred to herein as the object fingerprint, is derived by performing an MD5 hash calculation on the contents of the object file. The result of this MD5 hash calculation is a 128 bit string. For this embodiment, the DOSM file lookup table stores, in the file identification column, the 128 bit string, with the file designation "MD5." The second column of the DOSM file lookup table stores the IP address of the intelligent storage node that stores the object file (*e.g.*, "10.3.100.1"). The third column, labeled disk ID, stores an integer value that identifies the specific disk drive on the intelligent storage node that stores the object file. In one embodiment, when the look-up table is at full capacity, the DOSM uses a least recently used ("LRU") caching algorithm to replace existing entries in the DOSM lookup table with new entries received.

As shown in Figure 6, the DOSM also includes a data cache 620. In general, the data cache 620 stores objects (*i.e.*, client data) to permit the DOSM to streamline data directly to the recipient in response to a download request. During a download request, in the event of a cache miss, when the object is transferred from the intelligent storage node to the recipient, the object is also stored in the data cache 620. Similar to the DOSM file lookup table, the data cache 620 uses a least recently used ("LRU") caching algorithm to replace existing entries with new data objects when the data cache is full.

The DOSM also maintains a state table 630. In general, the state table 630 provides the state of the system by storing information on the overall capacity and health of the intelligent storage nodes 340. In one embodiment, the state tables are built using the multicast protocol to obtain, from the intelligent storage nodes, information about the corresponding intelligent storage node. The state information indicates whether disks on the

intelligent storage nodes are healthy, how much space is on the disks, etc. In one embodiment, as shown in Figure 6, state table 630 stores: read- write state of the storage nodes; health of the storage nodes (including an identification of failed nodes); and the current load of the storage nodes, including available storage capacity and number of input/output ("I/O") operations per second. The DOSM uses state information to select, in an upload operation, the appropriate intelligent storage node for storage of a new object file. For example, the DOSM uses information on the number of input/output ("I/O") operations per second to load balance the storage nodes. The DOSM also uses information on available storage capacity to select an intelligent storage node to store a new object file.

Figure 7 is a block diagram illustrating one embodiment for an intelligent storage node. For this embodiment, the intelligent storage node is implemented on a computer, including software to perform the functions described herein. An intelligent storage node 700 includes a processing core 710 that consists of one or more central processing units ("CPUs"). In one embodiment, the processing core 710 comprises two CPUs. The intelligent storage node 700 also includes volatile memory, labeled 730 in Figure 7. The memory 730 is used to store instructions executed by the processing core 710, as well as data used by the intelligent storage node. The intelligent storage node 700 further includes a network interface 720 to interface the intelligent storage node to the plurality of distributed object storage managers 320 via the interconnect fabric 330. The elements of the intelligent storage node 700 communicate via a computer transport mechanism 750 (*e.g.*, a peripheral component interconnect ("PCI") bus, processor bus, etc.). The computer transport mechanism 750 is intended to represent a broad category of one or more computer busses, such as peripheral component interconnect ("PCI") bus or the industry standard association ("ISA") bus.

The intelligent storage node 700 further includes a plurality of disk drives 740 to store the object files. As shown in Figure 7, the number of disks in an intelligent storage node is represented as "n", such that "n" is an integer value greater than one. In one embodiment, the processing core 710 communicates with the disk drives 740 using the ISA protocol. However, any protocol used to access the disk drive, including standard computer serial interface ("SCSI") protocol, may be used without deviating from the spirit or scope of the invention.

The intelligent storage node contains information to identify object files that it stores. In one embodiment, the information to identify object files is stored in the file system

directory of the intelligent storage node. In other embodiments, the information to identify object files is cached. Table 5 illustrates example entries to cache the identification of object files in an intelligent storage node.

Table 5

FILE ID	DISK ID
File1.MD5	1
File6.MD5	2
File4.MD5	2
File5.MD5	"n"

Table 5 includes a file identifier and a disk identifier. The file identifier, or file ID, stores the unique file handler corresponding to the object file. In one embodiment, the unique file handler is the object fingerprint obtained from performing an MD5 hash function on the contents of the object file. For the first example entry in Table 5, the unique file handler is represented as "file1.MD5." The second column, labeled disk id, identifies the specific disk drive on the intelligent storage node that stores the object file. For the second example entry in Table 5, the object file, "file6.MD5", is stored on the second disk drive on that intelligent storage node. On initial start-up of the intelligent storage node, the intelligent storage node builds the file identification table.

The storage cluster also processes upload requests. Figure 8 is a flow diagram illustrating one embodiment for processing upload requests in the storage cluster. For purposes of nomenclature, the "source", as used herein, refers to the source of the object file for the upload operation. If the storage cluster receives an upload request, then the load balancing fabric 320 (Figure 3) selects an available DOSM to process the upload request (blocks 805 and 810, Figure 8). The VFS creates a file identification (*e.g.*, storage system node) and the appropriate directory for the new object file (block 805, Figure 8). The selected DOSM parses the upload request to extract the certificate, object file, as well as client and directory information (block 820, Figure 8). If the upload request does not authenticate, then the DOSM transmits an error message to the source (block 835, Figure 8). Alternatively, if the upload request does authenticate, then the DOSM selects at least one intelligent storage node to store the object file (block 840, Figure 8). In one embodiment, the upload operation stores the object file in two storage nodes. The "mirroring" of the object

files ensures accessibility to the object in the event a failure occurs in an intelligent storage node. In one embodiment for "mirroring" the object files, the network storage system stores the object file at different geographic locations (*e.g.*, different storage centers). If access to the geographically disparate storage center is unavailable at the time the object file is uploaded, then an additional copy of the file is stored at the local storage center.

In one embodiment, the DOSM uses a state table (Figure 6) to select the intelligent storage nodes most appropriate to store the new object. For purposes of discussion, the selected intelligent storage nodes are referred to herein as the "destination intelligent storage nodes." The DOSM establishes a connection with the destination intelligent storage node (block 850, Figure 8). In one embodiment, the DOSM establishes a DOSP point-to-point connection with the destination source node. The object file is then transferred to the destination intelligent storage node (block 860, Figure 8). In addition, after transferring the file to the intelligent storage node, the DOSM receives a status message as part of the DOSP point-to-point protocol. The status message indicates whether the transfer operation was successful.

In one embodiment, the destination intelligent storage node generates a unique fingerprint for the object file (block 870, Figure 8). Specifically, the destination intelligent storage node computes an MD5 hash of the contents of the object file. The intelligent storage node also verifies the object file. After receiving the successful status at the DOSM, the DOSM establishes a connection to the virtual file system ("VFS"). The DOSM communicates file information (*e.g.*, the 128 bit.MD5 unique object fingerprint, file size, etc.), directory information (*e.g.*, folder ID, parent folder ID, etc.), as well as client information and metadata (block 880, Figure 8). The VFS attempts to verify the upload. If the VFS does not verify the upload, then an error message is sent to the source of the upload request (blocks 890 and 835, Figure 8). If the VFS does verify the upload, then the verification is transmitted to the DOSM. In turn, the DOSM verifies the upload to the source (block 895, Figure 8). Also, the storage system returns, to the source, a file handler that uniquely identifies the file to the network storage system.

If the source of the upload request is an end-user, then the DOSM re-directs the end-user to the client. For example, the DOM may redirect the end-user to a predetermined URL at the client's web site. In other embodiments, if the source was a storage port, then the DOSM transmits a storage system node (*i.e.*, handler used only for the storage system) and the unique object file fingerprint.

As discussed above, as part of the upload operation, the network storage system generates a unique fingerprint of the object file. Figure 9 is a flow diagram illustrating one embodiment for generating unique fingerprints of object files. First, the destination intelligent storage node creates a temporary file with the contents of the object file (block 900, Figure 9). An MD5 hash calculation is performed on the contents of the temporary file (block 910, Figure 9). The DOSM determines whether the unique fingerprint, generated from the MD5 hash operation, currently exists in the network storage system (block 920, Figure 9). If the fingerprint currently exists, the temporary file, which holds the contents of the object, is deleted (blocks 930 and 940, Figure 9). Also, a reference count associated with the existing fingerprint file is incremented (block 950, Figure 9). The use of reference counts is described more fully below in conjunction with a discussion of the delete operation. If the fingerprint generated from the temporary file does not exist, then the temporary file is converted to a permanent file, and the unique fingerprint is used to identify the file in the storage cluster (block 960, Figure 9).

Virtual File System:

In one embodiment, directory operations are performed in the virtual file system ("VFS"). Figure 11 is a block diagram illustrating one embodiment for implementing a VFS for use with a network storage system. In general, the VFS is the control path for maintaining the network storage system. The VFS maintains, for each object file, the customer file directory including the customer assigned filenames and the unique network storage system file identifiers. In one embodiment discussed above, the unique network storage system file identifiers consist of a 128 bit digital fingerprint obtained from performing an MD5 hash calculation on the contents of the object file. As shown in Figure 11, the VFS consists of distributed directory managers ("DDMs") 1110 and distributed directories 1120. There are "n" DDMs and "n" distributed directories, wherein "n" represents any integer one or greater. In one embodiment, each client is mapped to a distributed directory.

The DDMs support common directory operations, such as "open file", "move file", "delete file", "open folder", "move folder", and "create folder." The arrows of Figure 11 depict multi-directory requests and operations. The requests may originate from the end-user or the client, via a storage port or a web store. In one implementation, the requests to the VFS are transported using HTTP requests and encoded using the eXtended markup language

("XML"). Although the VFS is described using the HTTP protocol with XML encoded requests, any network protocol with any type of request format may be used without deviating from the spirit or scope of the invention.

In one embodiment, the VFS employs a database to implement the file system. For the database implementation, each directory operations request is converted into the database operation. Alternatively, the VFS may implement the file system using a local file system (*i.e.*, a file system local to the VFS). For the file system embodiment, files are generated to store information stored in the database implementation. Also, the DDMs include a lookup table to locate the files in the distributed directories. The files or database tables are replicated in a remote storage center.

The network storage file system consists of files arranged in directories or folders (hereafter referred to as folders). Similar to most file systems, the network storage file system is a hierarchical file system. In a hierarchical file system, directories or folders are arranged in levels, starting with a root or base folder. Additional folders or sub folders are then arranged under the root folder. The file system may comprise any number of levels, such that additional layers of sub folders fall beneath other sub folders. For purposes of nomenclature used herein, a parent folder to a folder is the folder arranged above the folder in the hierarchy of folders or directories.

Figure 12 illustrates example database tables for implementing the file system with a database. For the database embodiment, the VFS maintains a customer table 1200, folder table 1210 and file table 1220. The customer table 1200 includes fields for "customer ID", "customer name", and "customer reserved fields." The customer ID is a network storage system identifier used to uniquely identify the client. The customer name is the real name associated with a customer. For the first example entry in the customer table 1200, "customer A" has a customer ID of "1." The customer reserved fields provide storage reserved for use by the client.

The folder table 1210 includes fields for "customer ID", "folder ID", "folder parent ID", and "metadata." For this embodiment, each entry in the folder table corresponds to a folder in the network storage file system. The customer ID, the same customer ID stored in the customer table, uniquely identifies the client. For the example entries in folder table 1210, the customer ID of "3" identifies that the folders have been assigned to "customer C." The folder ID identifies the specific folder for that entry. For example, the first entry in folder table 1210 is for a folder identified by the identification of "2." The third column,

labeled "folder parent ID", identifies the parent folder for the folder corresponding to the database entry or row. For example, the second entry in folder table 1210 is a sub folder to the first entry of table 1210 (i.e., folder "100" is in the next hierarchical level beneath folder "2"). Note that the first entry in folder table 1210 does not have a value for the folder parent ID. This signifies that folder "2" is a root folder.

The file table contains an entry for each object file stored in a network storage file system. The example file table 1220 includes columns or fields for "customer ID", "file handler", "folder ID", "folder parent ID", and "metadata." Again, the customer ID identifies the customer that owns the file. The entries shown in file table 1220 are for files stored by customer C. The file handler field stores the fingerprint that the network file system uses to uniquely identify the file. Although the network file system stores 32 byte hexadecimal character sequences to identify files, for purposes of illustration, file handler entries for file table 1220 are shown as "52.MD5", "55.MD5", "99.MD5", and "67.MD5." The folder ID field identifies the folder that contains the file. For example, the first entry in file table 1220, corresponding to file "55.MD5", is organized or stored in folder 100. The folder parent ID identifies the parent folder to the folder that stores the file. The folder 100, which contains "52.MD5", has a parent folder of "2."

Figures 13A and 13B are flow diagrams illustrating one embodiment for performing directory operations in the VFS. When a DDM receives a directory operation request, the DDM parses the request to extract the certificate, an operational code, as well as arguments corresponding to the operational code (blocks 1300 and 1310, Figure 13A). The operational code specifies the directory operation requested. The DDM, using the certificate and the information contained in the request, validates the request. If the request does not validate, the DDM sends an error message to the requester (blocks 1320 and 1330, Figure 13A). Alternatively, if the request does validate, the DDM parses the operational code and extracts the arguments, including the folder to perform the open operation (blocks 1320 and 1330, Figure 13A).

In general, if the operation is for an "open folder" operation, then the DDM returns all sub folders and files contained in the folder identified by the argument. Specifically, the DDM extracts, from the appropriate distributed directory, the file and folder tables that correspond to the folder identified as an argument in the "open folder" request (blocks 1340 and 1345, Figure 13A). Specifically, the DDM extracts all the files and sub folders that correspond to the folder identified as an argument with the request. Using the example of

Figure 12, if the "open folder" request included the arguments "folder ID = 2" and "customer ID = 3", then the DDM extracts, from the folder table in the distributed directory, folder IDs 100 and 251 (*i.e.*, folders 100 and 251 are sub folders of the root folder 2). If the "open folder" request included the arguments "folder ID = 100", then the DDM extracts from the file table file handlers "52.MD5" and "55.MD5."

If the operational code in a directory request is for an "open file" operation, subsequent to an "open folder" request, then file information is obtained from the file table (*i.e.*, file handler) and the client table (*i.e.*, client identification) to construct an authentication certificate and an SRL for the file. For the above example, if the argument with the "open file" operation specified the file "52.MD5", then file and client information are obtained to construct the SRL for the "52.MD5" file.

If the operational code in a directory request is for a "move folder" operation, then a database operation is performed to revise the entries in the file and folder tables to reflect the new location of the folder. The "move folder" operation includes, as an argument, the new destination for the folder. Using the example of Figure 12, if the "move folder" operation specified moving folder ID 166 from a sub folder of folder ID 251 to directly beneath the root folder 2, then the parent folder ID on the fourth entry of folder table 1210 is modified from "251" to "2." Also, for file table 1220, the parent folder ID for the third and fourth entries are modified from "251" to "2."

If the directory operation is a "create folder" operation, then a new entry or row is generated for the folder table (blocks 1360 and 1365, Figure 13A). The "create folder" operation includes a parent folder as an argument. As described below, the client's folder name is converted to the network storage systems folder identification. Using the example of Figure 12, if the requester desires to create a new folder under the sub folder 166, then the DDM assigns a new folder identification for the folder, and enters a new row or entry for the folder table 1210 with a folder parent ID of 166.

If the directory operation is a "move file" operation, then a database operation is performed to revise an entry in the file table to reflect the new location of the file (blocks 1370 and 1375, Figure 13A). The "move file" operation includes a new destination for the file as an argument in the directory request. For the example database tables in Figure 12, if the "move file" operation specified moving file "52.MD5" from folder 100 to folder 166, then the folder ID and folder parent ID fields for the first entry of file table 1220 are revised to "166" and "251", respectively.

As shown in block 1390 of Figure 13A, the arguments extracted from the database tables are returned to the requester. In one embodiment, the response from a DDM includes XML encoded documents with the list of files (*i.e.*, in the form of a SRL) and/or directories. For example, in response to the "open folder" request, the VFS returns file and folder Ids for the files and subfolders arranged under the subject folder.

Figure 13B is a continuation of the flow diagram of Figure 13A illustrating additional file system operations in the VFS. If the operational code is a "delete folder" operation, then the corresponding folder entry is deleted from the folder table (blocks 1372 and 1374, Figure 13B). If the operational code designates a "delete file" operation, then the file entry, identified in the operation, is deleted from its file table (blocks 1376 and 1378, Figure 13B). For a "create file" operation, the VFS adds an entry for a new file in the file table (blocks 1386 and 1388, Figure 13B). If the operational code specifies an "update folder" operation, then the client metadata in the corresponding folder table for the folder entry is updated (blocks 1386 and 1388, Figure 13B). For an "update file" operation, the VFS updates client metadata in the table for the corresponding file entry (blocks 1392 and 1394, Figure 13B). After executing the appropriate database operation, the arguments for the operation are returned to the requester (blocks 1396, Figure 13B).

In one embodiment, the network storage system uses a reference count to manage up loading and deleting existing files. In general, when a new file is uploaded to the network storage system or a file request is received to upload an existing file, the reference count is incremented by one. Conversely, when a file request is received to delete a file, the reference count is decremented by one. The network storage system uses the reference count to delete an object file when the reference count is zero. For example, a client may transmit a first request to upload an object file, entitled "my file." After the upload operation is complete, the reference count to "my file" is one. Thereafter, a client may transmit a second request to upload "my file." Instead of storing a second copy of "my file", the network storage system increments the reference count of "my file" to "2." For this example, the client may then transmit a first request to delete "my file." In response to this request, the network storage system does not delete "my file." Instead, the network storage system decrements the reference count to "1." Thereafter, if the client transmits a second request to delete "my file", the reference count is decremented to "0", and the network storage system deletes "my file."

Figure 14 is a flow diagram illustrating one embodiment for the delete file operation for the network storage system. If the VFS receives a delete request, then a DDM performs a

validation check (blocks 1400 and 1405, Figure 14). If the delete request is not valid, then a error message is transmitted to the requester (blocks 1410 and 1415, Figure 14). If th request is validated, then the DDM extracts a file handler (*i.e.*, MD5 file handler) from th file table in the database (block 1420, Figure 14). The DDM deletes the file identificatio from the file table in the database (block 1450, Figure 14). In addition, the DDM constructs delete SRL, and transmits the delete SRL to the storage cluster (block 1460, Figure 14). I response to the delete operation, the storage cluster extracts the reference count for th corresponding file. If the reference count is greater than 1, the storage cluster decrements th reference count by one (blocks 1430 and 1440, Figure 14). Alternatively, if the referenc count is one, the storage cluster decrements the reference count to zero, and deletes the file identified by the SRL, in the appropriate intelligent storage node (block 1470, Figure 14).

Dynamic Data Caching:

Figure 10 is a block diagram illustrating one embodiment for caching data in th storage cluster. As shown in Figure 10, there are "n" DOSMs. Each DOSM (*i.e.*, DOSM 1 DOSM 2, DOSM 3 ... DOSM "n") contains a corresponding data cache (*i.e.*, data cache 1 data cache 2, data cache 3 ... data cache "n"). The network storage system file upload an download operations are received by the load balancing fabric 310 (also see Figure 3). A switch, such as an L4 switch, with load balancing capabilities, allocates resources among pool of resources. For the network storage system, the load balancing fabric 310 efficientl allocates requests among the "n" DOSMs. In one embodiment, when a DOSM transfers a object from the intelligent storage node to a destination, the object is cached in the data cach of the corresponding DOSM. Objects are deleted from the data cache in order to stor objects more recently requested via a least recently used ("LRU") caching policy.

Load balancing the DOSMs in the network storage system permits an "automatic' caching of objects in high demand. In prior art systems, elaborate mechanisms are employe to identify data in high demand. Based on these decision mechanisms, data is cached in a attempt to meet the needs of the high demand. For example, an object may be in hig demand when a movie studio offers, over its web site, a video preview of a newly released o upcoming film. For this example, the movie studio uses the network storage system t deliver the media rich object, "New Film Preview." The "New Film Preview" may b available to the end-user if the end-user "clicks" on a URL in the movie studio's web site For this example, if the movie is very popular, when the movie studio client offers the "New

Film Preview" through its web site, many end-users may attempt to download the rich object, "New Film Preview."

For an initial request to download the object "New Film Preview", the load balancing fabric 310 selects a DOSM to manage the request. For this example, the load balancing fabric 310 selects DOSM 1 to fulfill the request. Assuming the DOSM 1 does not currently store the object in its data cache, the DOSM 1 acquires the object from the appropriate intelligent storage node. As the object is delivered to satisfy the initial request, the object is stored in the DOSM 1 data cache 1. For this example, the storage cluster receives a second request for the "New Film Preview" object, and the load balancing fabric 310, based on availability, selects DOSM 3 to process the request. Again, assuming DOSM 3 does not currently store the object in its data cache, the DOSM 3 obtains the object from the appropriate intelligent storage node, and transfers the object to the requestor as well as stores the object in the data cache 3. Similarly, for this example, additional requests are made to the storage cluster to download the "New Film Preview" object. Based on available resources, the load balancing fabric 310 selects, for two separate requests, the DOSM 2 and the DOSM "n" to handle the two requests. Again, assuming DOSM 2 and DOSM "n" do not currently store the object in their data caches, both DOSMs acquire the "New Film Preview" object from the appropriate intelligent storage node, transfer the New Film Preview to the requestor, and store the object and their respective data caches (*i.e.*, data cache 2 and data cache "n"). As illustrated by the previous example, if an object is in high demand, the storage cluster, using a load balancing fabric that selects the different DOSMs, fetches, for storage in each of the DOSM data caches, a copy of the high demand object. Thus, the distribution of DOSM resources results in fast access to an object highly requested.

As shown in the example of Figure 10, each data cache stores potentially different objects depending upon requests processed in the respective DOSMs. For example, in addition to the "New Film Preview" object, data cache 1 stores "Photos Y" and "BLOB X"; data cache 2 stores "Ad 5" and "Video Snippet 8"; data cache three stores "Photos Z" and "Advertisement 10"; and data cache "n" stores "BLOB A" and "Video Snippet 2."

Geographic Replication of Storage Centers:

The network storage system is optimized to support a massive number of simultaneous download transactions. The network storage system relies upon a single virtual directory of all file objects. From any location on the Internet, clients see the exact same

view of their private file system. Thus, the network storage system supports simultaneous downloads of a single object that appears identical to users worldwide. In one implementation, the network storage system spans multiple continents with storage repositories or storage centers. The automatic geographic load balancing between storage centers ensures that all requests are directed to the nearest storage center. However, to provide fail over and enhanced performance, the storage center, including the storage cluster and VFS, are replicated. The physical replication across multiple locations includes a traffic management service. The traffic management service provides geographic load balancing of user transactions among geographic locations.

Figure 15 illustrates geographical replications of storage centers. For this example, there is a North American storage center 1510, an Asian storage center 1530, and a European storage center 1520. As shown in the example of Figure 15, clients and end-users in North America have optimal access to the storage center through the North American storage center 1510. Also, clients and end users in Europe have optimal access to European storage center 1520. Similarly, clients and end-users in Asia have optimal access to be Asian storage center 1530. In this configuration, the storage center is coupled to a wide area network to provide the maximum bandwidth for the delivery of objects. If a particular storage center becomes overloaded with requests, new requests are automatically diverted to the next closest storage center. All objects are geographically mirrored to provide one hundred percent disaster protection. Also, if access to the geographically disparate storage center is unavailable at the time a file is stored, then an additional copy of the file is stored at the local storage center (*i.e.*, the object file is mirrored locally).

The components within the network storage system are fully redundant with automatic recovery. Thus, the system supports extremely high level of service availability.

Download requests to each geographic storage center are continuously distributed across the DOSMs to deliver the fastest possible response time. In addition, in one embodiment, a global load balancing system ensures that the worldwide load across all storage centers is evenly spread to eliminate any "hot spots" and alleviate transitory demand spikes. The storage system operates far more quickly than the network itself, and thus introduces negligible delay to the overall file transit time. Thus, the worse case elapsed time for the individual object download is primarily determined by the speed of the wide area network used to transfer the object.

All components within the network storage system are replicated and redundant to provide complete recoverability in the event of a failure. In one embodiment, each storage center attaches to multiple network back bone providers to ensure continuous network access. All files and the control path directory structure are geographically replicated at the time of upload to prevent any possible loss of data. As is described more fully below, the system maintains coherency among disparate storage centers through use of the network storage replication protocol.

Figure 16 is a block diagram illustrating one embodiment for replicating the storage centers. For this example, two storage centers, labeled 1510 and 1520, are shown. However, based on the distributed architecture of the network storage system, any number of storage centers may be replicated. Storage centers 1510 and 1520 both include, for the storage cluster, load balancing fabric 320, distributed objects storage managers ("DOSMs") 320, interconnect fabric 330, and intelligent storage nodes 340. Storage center 1510 stores the same object files as storage center 1520. For example, if "object file 1" is stored in storage node 10 storage center 1510, then "object file 1" is stored in storage node "1" in storage center 1520. For the control path, the storage centers and 1510 and 1520 include the virtual file system ("VFS") 50. Similarly, the VFS in storage center 1510 stores the same directory information as the VFS in storage center 1520. Accordingly, the storage centers are replicated. Although the VFS and the storage clusters are shown in the same geographic "storage center", the VFS and storage cluster may be located at geographically disparate locations.

For this example, intelligent storage nodes in storage cluster 1510 (*i.e.*, storage node 1, storage node 2, ... storage node "n") are accessed via Internet protocol ("IP") addresses IP $addr_1$, IP $addr_2$, and IP $addr_n$, respectively. Thus, when a DOSM communicates with an intelligent storage node in storage center 1510, the DOSM uses these IP addresses to access the specific intelligent storage node. Storage center 1520 includes storage nodes (*i.e.*, storage node 1, storage node 2, ... storage node "n") addressed by IP address IP $addr_1'$, IP $addr_2'$, and IP $addr_n'$, respectively. Thus, in storage center 1520, when a DOSM communicates with the storage node, the DOSM uses an IP addr across the interconnect fabric 330. Although the replication of storage centers is described using an IP/TCP network protocol, any network protocol and corresponding addressing scheme may be used to replicate the storage centers.

As shown in Figure 16, the distributed objects storage managers of storage center 1510 or coupled to the interconnect fabric of storage center 1520. Similarly, the distributed

object storage managers of storage center 1520 are coupled to the interconnect fabric of storage center 1510. Based on this configuration, the distributed objects storage managers of storage center 1510 have access to the intelligent storage nodes of storage center 1520. Likewise, the distributed object storage managers of storage center 1520 have access to the intelligent storage nodes of storage center 1510. As discussed above, each DOSM maintains a lookup table that correlates a file to an IP address (See Figure 6). For example, if a file specified in a download request resides on storage node 1 in storage center 1510, then an entry of the DOSM lookup table specifies IP $addr_1$. Similarly, in storage center 1520, if a file resides in storage node 1, an entry for the DOSM lookup table specifies IP $addr_1$'.

The storage center architecture supports a "dynamic" fail over. If a storage node, or a disk drive on a storage node, renders the access to a file inaccessible, then the DOSM may obtain the file from the replicated storage center. In one embodiment, to perform "dynamic" fail over, a mapping is stored between intelligent storage nodes in storage center 1510 and intelligent storage nodes in storage center 1520. Table 6 below shows a mapping for the example in configuration of Figure 16.

Table 6

IP Address	**IP Address'**
IP $Addr_1$	IP $Addr_1'$
IP $Addr_2$	IP $Addr_2'$
...	...
IP $Addr_n$	IP $Addr_n'$

For this example, IP $addr_1$ maps to IP $addr_1'$. If there is a failure in storage node 1 in storage center 1510, then DOSMs of storage center 1510 access storage node 1 of storage center 1520 using IP $addr_1'$. In one embodiment, the IP mapping between storage centers is implemented by modifying only the subnet address portion between the two IP addresses mapped. For example, if IP $addr_1$ is 10.3.100.1, then IP $addr_1'$ is derived by changing, as appropriate, the subnet portion of the address (*e.g.*, 10.10.100.1).

The directory information stored in the VFS is replicated between storage center 1510 and 1520 in a similar manner. Thus, if a failure occurs in a distributed directory of storage center 1510, then the distributed directory manager in storage center 1510, using an IP address mapping, accesses the replicated distributed directory in storage center 1520.

In one embodiment, to further implement geographic application for a fail over mode, if one disk fails, then a DOSM attempts to identify the file in the same node at a different storage center. If a storage node is rendered inoperable, then the DOSM clears the entry in the DOSM file lookup table, and attempts to locate the file at a remote storage center. For example, if disk "2" of storage node "1" in storage center 1510 fails, a DOSM 320 attempts to locate the file in storage node "1", disk "2", in storage center 1520. If the file is not located in storage node "1", disk 2, of storage center 1520, the DOSM, using the multicast protocol, attempts to locate the file locally (*i.e.*, in the storage center 1510). If the file is not located locally, the DOSM, using the multicast protocol, attempts to locate the file at a remote storage center (*e.g.*, storage center 1520).

Accessing The Network Storage System:

The network storage system has application for use in content delivery networks. In general, content owners and providers often employ the services of a content delivery network. Content delivery networks attempt to optimize the delivery of commonly accessed rich media objects. In order to maximize the delivery of the rich media objects, content delivery networks employ local caches at the edges of the wide area network.

The network storage system has applications to complement content delivery networks by providing the underlying content for the content origin web site. In one embodiment, each cache at the content delivery network directly accesses the geographically closest storage center to locate the desired object to eliminate the need for content delivery network to access the content owner's/provider's web site.

Figure 17 illustrates one embodiment for use of the storage center in a content delivery network. For the example of Figure 17, the content delivery network 1700 includes an end-user computer 1740 coupled over a network (*e.g.*, Internet) to a content origin web server 1720. The content origin web server 1720 implements or hosts a web site. The web site permits the end-user to select content, such as rich media objects. A content delivery network includes a ("CDN") server 1730. The CDN server 1730 delivers content published on the web site by the content origin web server 1720. Specifically, the end-user computer 1740 is coupled to the CDN server 1730 to maximize the delivery of content, including rich media objects associated with the web site, to the end-user. The CDN server 1730 caches, at the CDN, a portion of the content associated with the web site 1730.

For purposes of illustration, a wide area network 1750 is shown as including satellite communication networks 1760, wireless communication networks 1770, and fiber-optic networks 1780. As illustrated in Figure 17, the CDN server 1730 is located close to the edges of the wide area network 1750. The location of CDN server 1730 close to the wide area network 1750 optimizes the delivery of objects cached at the CDN server 1730. For this embodiment, one or more storage center(s) 1710 are coupled to the CDN server 1730. In the event of a cache miss at the CDN server 1730, the CDN server 1730 obtains the content (*e.g.*, object file) from storage center(s) 1710. This configuration allows the CDN server 1730 to bypass the slower content origin web server 1720 in the event that content, requested by end-user computer 1740, is not located at the CDN server 1730. According, the storage center(s) 1710 optimize routing of content through the Internet back to the CDN when the desired content is not located in the local cache.

Figure 18 is a flow diagram illustrating one embodiment for use of the storage center with a content delivery network. The end-user, through the end-user computer, generates an HTTP request to the content origin web server (block 1800, Figure 18). In response to the user request, the content origin server returns to the end-user computer HTML with embedded file URLs (block 1810, Figure 18). The embedded file URLs identify the rich media objects stored at the CDN server. To obtain the rich media objects, the end-user computer generates HTTP file requests to the content delivery network (*e.g.*, CDN server 1730) (block 1820, Figure 18). If the file identified by the URL is located in a cache at the CDN server site, then the CDN server delivers the file to the end-user computer (blocks 1825 and 1850, Figure 18). Alternatively, if the file is not cached at the CDN server site, the CDN server generates an HTTP file request to the storage center (blocks 1825 and 1830, Figure 18). In one embodiment, the HTTP file request includes the network storage system's SRL, to uniquely identify the file. In response to the CDN server's request, the storage center downloads the file to the CDN cache (block 1840, Figure 18). The CDN server delivers the file to the end-user computer (block 1850, Figure 18).

Accessing The Network Storage System:

There are multiple ways to access the network storage system. In one embodiment, the client uses a "storage port." The storage port provides access to the network storage system through a standard file system interface (*e.g.*, network file system ("NFS") or Microsoft NT CIFS). The storage port may be configured by the client in various ways for

different applications to optimize the delivery of rich media objects. In one embodiment, the storage port is configured at the client site to provide seamless integration from the client site to the network storage system. In another embodiment, to further off load rich media object traffic from a web site, the storage port may be used as a file system manager that downloads files to the end-user directly from the network storage system. In other embodiments, the network storage system may be directly interfaced with a private file structure.

1. Storage Port Access:

The storage port device provides a transparent gateway connection into the network storage system. In one application, the storage port device is installed at the client site, and interfaces to local web servers via standard NFS or CIFS protocols over a local area network ("LAN") connection. Specifically, in one embodiment, the user mounts the storage port as a storage device on the client network. In this configuration, the storage port effectively provides the user with a virtual NFS or CIFS file system with storage capacity at the storage center (*i.e.*, provides the user with hundreds of terabytes in storage capacity). In one embodiment, the storage port device occupies only approximately 1.75 inches of rack height. As described more fully below, multiple storage ports may be installed at a single client site to increase aggregate throughput.

Figure 19 illustrates one embodiment for use of the storage port in the network storage system. An end-user 1900 communicates with a client site 1910 over a wide area network 1920. The end-user computer 1900 generates requests (*e.g.*, HTTP requests) for files accessed through the client's web site. A content web server 1925, located at the client site 1910, processes requests to the client web site, including requests to download rich media objects. Content web server 1925 is intended to represent a broad category of computers and software used to implement a web site, such as multiple web servers and/or application servers, and any hardware/software configuration may be used without deviating from the spirit or scope the invention.

The content web server 1925 is coupled to the storage port 1930 over a network, such as a local area network at the client site 1910. Specifically, the content web server 1925 generates file and directory operation requests in accordance with the format of the "local" file system. As used herein, a "local" file system connotes one or more file systems or file structures used at the client site. For example, the content web server 1925 may generate NFS or Microsoft NT CIFS requests for files and directory operations. To interface the

storage port 1930 with the content web server 1925, the storage port 1930 is mounted as a storage device. In one embodiment, one directory is mounted for object files and a second directory is mounted for SRLs. As shown in Figure 19, the storage port 1930 communicates with the storage center 1950 to conduct file and directory operations.

Figure 20 is a flow diagram illustrating one embodiment for use of a storage port to deliver content. The client site receives a URL file request from an end-user computer (block 2010, Figure 20). The URL identifies an object file associated with the client's web site. In response to the end user's URL file request, the client site (*e.g.*, content web server) generates a local file system request for the object file (block 2020, Figure 20). The local file system request is received by the storage port. The storage port includes a cache to store both object files and directory information. If the object file is stored locally in the storage port, then the storage port retrieves the object file from the data cache, and returns the object file to the content web server in response to the local file system request (blocks 2030, 2040, and 2070, Figure 20). Alternatively, if the storage port does not store a copy of the object file in its data cache, then the storage port requests the object file from the storage center (blocks 2030 and 2050, Figure 20). In response to the local file system request, the storage center downloads the object file to the storage port, and the object file is returned to the content web server (blocks 2060 and 2070, Figure 20). Thereafter, the content web server delivers the object file to the end-user in response to the URL file request (block 2080, Figure 20).

The storage port may be implemented in either hardware or software. Figure 21a illustrates one hardware configuration for a storage port device. As shown in Figure 21a, the content web server 2100 communicates with the storage port 2110 over a communications link 2120, such as a local area network. The storage port 2110 conducts file and directory operations with storage center 2130.

Figure 21b illustrates embodiments for implementing the storage port in software. In one embodiment, the network storage system is accessed through library calls or through application program interface ("API") calls. For these embodiments, the software provides translation between the client's local file system and the network storage file system. As discussed above, the storage center 2160 includes software running on computers for performing the functions of the VFS and intelligent storage clusters. This software includes entry points (*i.e.*, APIs) to permit interfacing of external software. In part, the APIs on the storage center software permit the client to conduct file and directory operations as described herein. As shown in Figure 21b, content web server 2140 runs, in addition to software to

operate the client site, software to call APIs in the network storage center. Thus, for this embodiment, the content web server 2140 executes network storage system file and directory operations over the wide area network 2180 through remote program calls.

In another embodiment, shown as storage system library calls 2155, a customized network storage system library includes a collection of file system operations. For example, one library function may permit software operating at the client (*e.g.*, on content web server 2140) to request an object file download to the storage center through use of the library function. For this example, to perform the file download operation, the client software calls the file download function and passes the SRL as an argument to the function call. A library of functions provides an additional means to interface client software to directly access the network storage system.

Figure 22 is a block diagram illustrating one embodiment for a storage port. As shown in Figure 22, a storage port 2200 includes a processing core 2210, memory 2230, storage port data store 2240, and network interface(s) 2220. These components are coupled via a bus transport 2250 that may include one or more busses (*e.g.*, ISA, PCI, or microprocessor buses). Processing core 2210 includes one or more central processing units ("CPUs"). In one embodiment, the storage port includes two CPUs. Memory 2330 is used to store, during operation of the device, software to perform the functions of the storage port described herein. The storage port data store 2240 contains one or more hard disk drives (*i.e.*, "n" hard disk drives, wherein "n" is any number one or greater), used, in part, to cache file system information (*i.e.*, directory cache) and object files (*i.e.*, data cache). The network interface(s) 2220, which includes "n" network interface cards, couples the storage port 2200 to client devices (*e.g.*, content web server). In addition, to support a fail over architecture, the network interface cards are used to connect one or more storage ports together. In one embodiment, the storage port includes three network interface cards.

Figure 23 is a block diagram illustrating one embodiment for file system translation in the storage port. The network storage system issues "file handlers" unique to the network storage system. In one embodiment, a network storage system file handler identifies, for a corresponding file: a) client identification; b) parent directory; c) metadata and d) the unique digital fingerprint (*i.e.*, 128 bit MD5 identification). In general, the file system translation software 2300 converts local file system operations to network storage system file system operations. In one embodiment, to perform this function, the software includes file system

translator 2320 and storage system access processes 2330. The file system translator 2320 includes local file system interception 2340 and storage system kernel processes 2350.

In operation, local client file system 2310, which may include operating system software running at the client's site, issues local file system operations. For example, the client software may issue requests, in accordance with UNIX or Microsoft NT to open a file. The file open operation includes a file descriptor that identifies the file in the local file system. Typically, file system calls are processed by the operating system kernel (labeled 2360 in Figure 23). The operating system kernel software maintains a mapping between file descriptors and directories to "inodes." The inodes provide the system a physical pointer to the file data in the system (*e.g.*, a pointer to the file stored on a hard disk drive).

For the embodiment of Figure 23, when the local client file system 2310 issues a file system operation, local file system interception 2340 "traps" or intercepts the call, and passes the thread of execution to the storage system kernel processes 2350. In one embodiment, the local file system interception 2340 comprises CODA software, developed at Carnegie Mellon University. In general, CODA is a type of distributed file system. A portion of the functionality provided by the CODA software exports an underlying file system. Specifically, CODA exports file system operations, typically executed in the kernel level, to applications programs accessible in the user portion of memory. Although file system translation is described using CODA to intercept local file system operations, any software that intercepts file system calls may be used without deviating to the spirit or scope of the invention.

In general, the storage system kernel processes 2350 obtains network storage system file handlers (referred to herein as "storage handlers") for storage in operating system kernel 2360 to provide a mapping between local file system descriptors and storage handlers. Thus, the file descriptors provide a handle to identify files and directories in the local file system, and the storage handlers provide a handle to identify files and directories in the network storage system.

To maintain the mapping between local file system descriptors and storage handlers, the storage system kernel processes 2350 obtains network storage file system information from storage system access processes 2330. Specifically, storage system kernel processes 2350 obtains from storage system access processes 2330 storage handlers and directory information. As shown in Figure 23, storage system access processes 2330 obtain directory and storage handler information from directory cache 2370. Alternatively, if directory and storage handler information is not cached at the storage port, storage system access processes

2330 query the network storage system (*i.e.*, VFS) to obtain directory information and storage handlers. Accordingly, the translation system 2300 provides a mapping between the client's local file system and the network storage file system.

Figure 24 is a flow diagram illustrating one embodiment for translating a file system operation from a local file system to the network storage file system. The process is initiated by the client issuing a local file system request (block 2400, Figure 24). The local file system request is received by the operating system kernel, and dispatched to the file system translator (Figure 23). For example, if the file system operation is an open file operation for the file "foo.txt", then the operating system kernel dispatches the open file operation with the file name "foo.txt" as an argument to the file system translator. If the file system operation is an "Open Folder" operation for the folder "dir1", then the operating system kernel dispatches the open folder operation with the folder name "dir1" as an argument.

The process determines whether there is sufficient directory information in the storage port directory cache (block 2430, Figure 24). For the "Open Folder" example above, if the storage handlers for all subfolders and files are not stored in the directory cache, then additional directory information is required to fulfill the request. For the "Open File" example, if the storage port has been recently initialized and thus does not contain information on the file, then additional directory information on the file (*e.g.*, "foo.text") is required to open the file.

If there is sufficient directory information in the directory cache, and the file system operation does not require retrieving data (*i.e.*, the file system operation is not an "open file" operation) or updating directory information, then the appropriate directory information from the directory cache is retrieved and returned in response to the local file system operation (blocks 2430 and 2435, Figure 12) (blocks 2435 and 2437, Figure 24). For the "Open Folder" example above, storage handlers for all subfolders and files in the subject folder are retrieved from the directory cache, the storage handlers and corresponding file identifiers are stored in the operating system kernel, and the file identifiers are returned to local file system.

If additional directory information is required (*i.e.*, the information is not in the storage port directory cache), then a request is generated to the VFS for the additional directory information (block 2070, Figure 24). In one embodiment, the storage port generates an XML encoded request. For the "Open Folder" example, if the storage nodes and corresponding file identifiers are not stored in the directory cache, then the storage port generates an XML encoded "Open Folder" request to extract file and folder information for

files and subfolders within the subject folders (*i.e.*, the folder that is the subject of the "Open Folder" request). In one embodiment, in response to a request for folder information, the VFS returns name, folder identification, client metadata, upload SRL, and parent folder identification. In response to a request for file information, the VFS returns name, file identification, client metadata, download SRL, and parent folder identification. In one embodiment, the client metadata fields are used to track and maintain state information used in the local file system (*e.g.*, information for UNIX, Microsoft Windows or NT, etc.). In addition to obtaining additional directory information, if the client local file system command is a directory operation (*i.e.*, "move folder", "delete folder", etc.), then an XML request to the VFS is generated to perform the directory operation in the VFS. The directory information is received and stored in the directory cache (block 2480, Figure 24).

If the file system operation requires file data (*e.g.*, open file, read file etc.), then the storage port determines whether the file is located in the data cache (block 2440, Figure 12). If the file is stored in the data cache, then the file, or appropriate portion, is transferred from the storage port to the client requestor (block 2090, Figure 12). Alternatively, if the file is not in the data cache, then the storage port generates a file download request to the storage cluster (block 2050, Figure 24). In response to the storage cluster request, the storage port receives and subsequently caches the object file in the data cache (block 2060, Figure 12). The object is then transferred from the storage port to the client requestor (block 2090, Figure 12).

2. End User Network Storage System Access Method:

In another embodiment, the storage port supports file downloads directly to the end-user or through a CDN partner. In one embodiment, the SRLs are directly embedded into the Web page HTML, and are sent to the end-user. This results in transferring objects directly from the storage center to the end-user browser. Figure 25 is a block diagram illustrating one embodiment for using the storage port to directly download object files to the end-user. For this configuration, an end-user computer 2610 communicates with a client site 2620 and the storage center 2650. The client site 2620 maintains a web site. For this embodiment, the client site 2620 maintains a web site through a content web server 2630. However, any configuration of servers, including remote web site hosting, may be used without deviating the spirit or scope of the invention.

The content web server 2630 communicates with the storage port 2640, and in turn, the storage port 2640 communicates with the storage center 2650. As illustrated in Figure 25,

the end-user, through end-user computer 2610, generates URL requests to the client site 2620, and receives, in return, HTML with one or more embedded SRLs. Using the embedded SRLs, the end-user computer 2610 generates SRL requests directly to the storage center 2650 over a wide area network 2660. In response, the storage center 2650 serves object files directly to the end-user computer 2610.

Figure 26 is a flow diagram illustrating one embodiment for directly downloading object files to an end-user. The client site (*e.g.*, content web server) generates local file system requests for SRL(s) corresponding to file(s) (block 2700, Figure 26). The file(s) contain content that the client desires to embed in the web page. In one embodiment, the storage port dynamically generates the SRL(s) in response to the request from the content web server (block 2710, Figure 26). In one embodiment, a time-out parameter is added to the SRL(s) (block 2720, Figure 26). The time-out parameter permits a client to specify a period of time that the SRL is valid (*i.e.*, a period of time that the end-user may access the file). In one implementation, the time-out parameter specifies a period of time with a granularity in seconds.

The SRL(s) are embedded in the HTML of the client's web page (block 2730, Figure 26). The end-user issues web page requests to the client site (block 2740, Figure 26). The content web server then downloads the requested HTML with the embedded SRL(s) (block 2745, Figure 26). With the embedded SRL, the end-user generates HTTP requests to the storage center (block 2750, Figure 26). If the SRL(s) do not authenticates\ at the storage center, then the storage center transmits an error message to the end-user (block 2755, Figure 26). If the SRL(s) do authenticate, then the time-out parameter is checked to determine whether the file access is valid (block 2760, Figure 26). If the SRL is not valid (i.e., the time-out parameter is out of range), then the operation is ceased (block 2760, Figure 26). If the SRL is within the specified time range, then the storage center downloads the object file to the end-user (block 2770, Figure 26).

The storage port 2640 acts as a file system cache. For this embodiment, the storage port contains the client's SRL files stored in a standard NFS or CIFS directory format. Each NFS or CIFS file contains the corresponding SRLs, and the SRLs contain the unique file identifier and the SRL authentication certificate.

In one embodiment, to deliver the SRLs to the end-user, the network file system utilizes a second directory, in addition to the directory for the object files, that shadows the object file directory. The client uses the second directory to obtain shadow files. A shadow

file contains an SRL to identify an object file of the network storage system. In one embodiment, to embed the SRL into the web page HTML, the client reads the contents of the shadow file for the corresponding object file. In one embodiment, the shadow file is generated during an upload operation. The client may access a shadow file by mounting the second directory. For example, a client may specify, for the file "foo.text", the following directory-filename:

storagefilesystem:/export/dir/foo.text.

The client uses this directory and filename to access the contents of the object file, "foo.text." To obtain the SRL for the example file "foo.text", a client mounts a different directory, such as the following example directory:

storagefilesystem:/SRL/dir/foo.text,

wherein, the SRL file contains a unique file identifier and the SRL authentication certificate for the file, "foo.text." To deliver the SRL to the end-user, the client reads the contents of a shadow file for the corresponding object file, and publishes the SRL to the user.

3. Client Private File System Directory:

The network storage system of the present invention also supports using an existing private file directory to access the storage system. For this embodiment, the network storage system customer (*e.g.*, client) may desire to use their own file structure in conjunction with the network storage system's file system. In other embodiments, a client of the network storage system may wish to develop a file system to track additional information beyond that information tracked using NFS or CIFS.

Figure 27 is a block diagram illustrating one embodiment to interface a storage center to a client's private file directory system. In one embodiment, the storage port at the client site 2820 is replaced with a private file manager 2840. For this embodiment, the private file manager 2840 generates SRLs for object files using a unique file identification assigned to the user file at the time of upload, as well as using a shared secret to authenticate file system operations. As shown in Figure 27, the content web server 2830, operating at the client site 2820, generates file system requests to the private file manager 2840. In turn, the private file manager 2840 issues SRLs corresponding to the object files that are the subject of the request. In one embodiment, the client supplies their own unique ID at the time the client

uploads files to the storage center. In another embodiment, the client utilizes, in requests to download files, the object finger print returned by the storage center.

As shown in Figure 27, the end-user, through end-user computer 2810, generates URL requests to the client's web site. In turn, the client site 2820 returns HTML with embedded SRLs. With the embedded SRLs, the end-user computer 2810 generates SRL requests, over a wide area network 2860, to the storage center 2850. In turn, the storage center 2850 serves object files identified by the SRL.

Figure 28 is a flow diagram illustrating one embodiment for accessing object files in a storage center using a client's private file system. The end-user issues the URL requests to the client web site (block 2900, Figure 28). In response, the client (*e.g.*, content web server) generates file location requests to a file manager (block 2910, Figure 28). In general, the file manager services requests to issue SRLs corresponding to files in the client's private file system. A client may use any type of file system in conjunction with the network storage system. All that is required is that the client's private file system issues SRLs for files managed by the client's private file system. The file manager retrieves the SRL for the file associated with the HTML, and delivers the file to the content web server (block 2920, Figure 28). The content web server then transmits to the end-user HTML with the embedded SRL (block 2930, Figure 28). Thereafter, the end-user generates HTTP requests to the storage center with the SRL (block 2940, Figure 28). If the SRL does not authenticate, then the storage center issues an error message to the user. Alternatively, if the SRL authenticates, then the storage center generates an MD5 hash on the client supplied unique file ID to identify the file (block 2947, Figure 28). The storage center thereafter downloads the object file to the end-user (block 2950, Figure 28)

For the client's private file system access method, the client maintains a mapping between unique filenames and SRLs. In one embodiment, the unique filename is not obtained from an MD5 hash operation, but is a unique filename. Thus, the network storage system utilizes a technique to differentiate between MD5 file names, derived from the contents of the object file, and client unique file names. In one embodiment, to differentiate between these two types of file names, the network storage system assigns different storage fingerprint identifiers. For a filename generated by an MD5 hash operation on the contents of the object file, the file is designated "128bits.MD5." To identify a customer unique filename, the file is designated as "MD5.UFID" (*i.e.*, where "MD5" is the client's unique file name). This convention permits the network storage system to differentiate between the twp types of

file identifiers, and allows the customer to interface with the network storage system by only designating unique file names.

Failover Architecture:

In one embodiment, the storage port supports failover or failsafe architectures. Figure 29 is a block diagram illustrating one embodiment for a storage port fail over configuration. For purposes of explanation, Figure 29 illustrates a fail over configuration with two storage ports. However, the storage port fail over configuration may be extended to any "2N" fail over configuration. For this embodiment, the fail over configuration includes an active storage port 3010 and a passive storage port 3020. Each storage port includes a plurality of network interface cards. Both the active storage port 3010 and passive storage port 3020 communicate to storage center(s) over wide area network 3065, through network interface cards 3045 and 3025, respectively. The active storage port 3010 and passive storage port 3020 also communicate to the client site network via network interface cards 3050 and 3035, respectively. As shown in Figure 29, the client accesses the active storage port 3010 over client site network 3060 using IP Addr.

For the embodiment of Figure 29, a third network interface card is contained on both the active storage port 3010 (3055) and passive storage port 3020 (3030) to communicate between the devices for fail over monitoring. The active storage port 3010 operates as current storage port at the client site. The passive storage port 3020 monitors the health of the active storage port 3010. Specifically, active storage port 3010 includes health monitoring 3070 that continually executes a process to ascertain the health of the active storage port 3020 (*e.g.*, health of the CPUs, hard disk drives, etc.). For this embodiment, the passive storage port 3020 queries the active storage port 3010 for health status. If a condition occurs in the active storage port 3010 that warrants a fail over condition, then the passive storage port 3020 becomes the active storage port (*i.e.*, the passive storage port is used to interface the client site to storage center(s)).

In one embodiment, to support fail over, one IP address is used for the NFS/CIFS export. For this embodiment, a standard IP switch over scheme may be utilized. Specifically, when a fail over condition occurs, the passive storage port 3020 assumes the IP address of the active storage port 3010. The health monitoring 3070 and 3080 include both active and passive processes, so that if a fail over condition occurs, the passive storage port may execute the active storage port process.

Figure 30 is a flow diagram illustrating one embodiment for a storage port fail over process. When a storage port fail over occurs, the new storage port does not contain any directory information in its directory cache or any objects in its data cache. Thus, after a fail over operation, if a file is open and the storage port receives a read file request, the new storage port must execute a file open operation (blocks 3130 and 3140, Figure 30). After the storage port receives the file identification information (*e.g.*, SRL), the storage port generates a request to the storage center to obtain the object file, in order to transmit a block of object data in response to the read file request.

After fail over condition, when a file is requested (block 3120, Figure 30) or an open file operation is necessary, the storage port generates an XML to the VFS to obtain file identification information (block 3150, Figure 30). In response, the VFS returns file identification information (block 3160, Figure 30). With the file identification information, the storage port updates its directory cache (block 3170, Figure 30). With the file identification information (*e.g.*, SRL), the storage port generates a request to the storage center for the object file (block 3180, Figure 30). In response, the storage center delivers the object file, and the storage port updates its data cache (block 3190, Figure 30). If the storage center download operation was in response to a read request to the storage port, the read request delivers data as specified in the read request.

Network Storage System Dynamic Failover:

In one embodiment, storage nodes monitor the health of their respective nodes (*e.g.*, monitor hard disk drives, processor, network access, etc.). If the health of a storage node requires that the storage node should cease operation, then the storage cluster executes a fail over operation. In one embodiment, in a fail over operation, the storage node reports the failed status to the DOSMs, and the DOSMs update their state table. If this occurs, the DOSMs attempt to locate the replicated file at a different storage node (*i.e.*, either locally for remotely).

Figure 31 is a flow diagram illustrating one embodiment for using the multicast protocol after a storage node fail over condition. If a storage node fails, then the DOSMs update and their state tables to indicate that the storage node is no longer in use (blocks 3210 and 3220, Figure 31). If the DOSM receives a file request for a file previously stored on the failed storage node, then the DOSM, which received the download request, issues a multicast protocol request to storage nodes (blocks 3225 and 3230, Figure 31). In one embodiment, the

DOSM may issue the multicast protocol request to local storage nodes (*i.e.*, storage nodes located at its storage center).

Each storage node that receives the multicast request determines whether it contains the requested object file (block 3240, Figure 31). If none of the storage nodes contain the object file, then the DOSM may issue another multicast protocol request at a remote storage location (blocks 3245 and 3247, Figure 31). Again, at the remote storage center, each storage node determines whether it contains the requested object file (block 3240, Figure 31). In another embodiment, if the DOSM does not locate the file using the multicast protocol, the DOSM may query each individual storage node using the DOSP point-to-point protocol.

When a storage node locates the requested object file, the storage node broadcasts the file identification information using the multicast protocol (block 3250, Figure 31). Each DOSM snoops, using the multicast protocol, to receive the file identification information (block 3260, Figure 31). As illustrated in the process embodiment of Figure 31, the multicast protocol may be used to synchronize file location information in the DOSMs in the event of a fail over condition.

Multi-Cast Protocol:

The multi-cast protocol of the present invention supports the maintenance of file information in a distributed storage system. Since the network storage system consists of a plurality of storage nodes, the multicast protocol is used to track file information and synchronize file information throughout the network storage system. The tracking and maintaining of file and directory information includes maintaining information throughout geographically disparate storage centers. In one embodiment, the multi-cast protocol synchronizes cache information in the DOSMs. For example, if a new object file is loaded, the multi-cast protocol provides a means for all DOSMs in the network storage system to obtain information necessary to access the new object file. In addition, some file operations, including delete file or update file operations, require updating the DOSM lookup tables. Also, if a storage node fails, and a fail over condition is executed, the multi-cast protocol provides a means for the DOSMs to locate the file at the storage node the file has been replicated.

The Distributed Object Storage Protocol (DOSP):

In one embodiment, the DOSP includes daemon/master services and multicast-based monitoring communications. Communication between the daemon and master components is accomplished through a set of "request packets" and "response packets." The request packets consist of three major subcomponents: an opcode that specifies the type of request; a header implemented via a C++ specific structure that provides information about the data that follows; and data transmitted, if any.

Each operation has an associated operation code and a pair of structures: one for issuance of the request, and a second separate structure for return values. Once the receiver has received and processed the request (sent data, deleted file, etc) it then sends a response consisting of the appropriate "Out Structure" indicating the status of the request (SUCCESS, FAILURE, etc) and any required return values. Currently, there are six service operations supported by the DOSP: null, store file, retrieve file, retrieve file range, delete file, and get contents.

The null operation provides a framework to develop future modifications of the protocol and to test basic functionality of the master/daemon request/response interaction.

When a file is ready for storing, the DOSM client sends a request id, followed by a request header. It then sends the data to the dosd in a series of chunks, each of which is preceded by a DosdStoreHeader which gives the size of the next chunk to be read, and a field indicating whether this is the last packet to be sent.

When a file is being retrieved from the Storage Cluster, the DOSM client sends a request Id, followed by a request structure. The DOSD responds by first sending the size of the data, the data requested, and finally an Out structure with the return value of the operation.

The get contents operation is used to acquire the contents of the storage node as a character based stream. The after the "In Structure" is passed to the dosd, the dosd first returns the length of the stream of md5 hash/node&disk associations, followed by the stream of data, with the "Out structure" coming last.

The DOSP provides an extensible framework for any new services or additional functionality. There are essentially three steps to adding new functionality: defining a new pair of In/Out structures; assigning a new opcode, implementing a handler in the DOSM client; and adding a service handler for the dosd.

To facilitate gathering of information about the system, the DOSP provides several multicast-based services. In one embodiment, these services work in a manner very similar to the non-multicast aspect of the protocol. Specifically, requests consist of three parts: an opcode; a request In structure; and any additional data.

Responses consist of a response structure containing a RETURN value and any other return values required to satisfy the request. If data is streamed, a size field precedes the data, followed by the data, and then followed by the Out structure.

Since multicast traffic occurs on a completely separate port from point-to-point dosm/dosd traffic, the multicast In/Out structures are not multicast-specific. This makes it possible for the DOSM to query the entire dosd storage cluster or to query an individual machine with the same request/response structures and their associated operational sequencing.

One of the jobs of the DOSM is to monitor the current state of nodes in the cluster. There are several tools to facilitate this task. Primarily, the various dos daemons multicast heartbeats on a specific multicast port and group. The DOSM contains an option to query a specific disk, or all of the disks on a given a storage node. A "get disk state" function returns a value, and an array of disk state values (online, offline, down) with one entry per disk. A "get disk status" function contains an option to query a specific disk, or all of the disks on a given a node. The "get disk status" contains a RETURN value, and an array of disk statistics; one array per statistic (bytes free, bytes available, inodes used, inodes available, number of outstanding ops), with one entry per disk. The DOSP includes a load balancing function.

The DOSP includes a heartbeat function. This allows querying specific machines for a heartbeat in addition to providing system-wide tracking functionality via multicast methods.

Although the present invention has been described in terms of specific exemplary embodiments, it will be appreciated that various modifications and alterations might be made by those skilled in the art without departing from the spirit and scope of the invention.

CLAIMS

What is claimed is:

1. A method for downloading a file from a remote storage center to an end-user computer for content provided from a content server, said method comprising the steps of:

receiving a request from an end-user computer for content at a content server;

transmitting from said content server to said end-user computer, in response to said end-user request, said content comprising at least one storage resource locator ("SRL"), wherein said SRL comprises a unique file identifier to identify a file associated with said content;

transmitting a request for said file from said end-user computer to a remote storage center, including transmitting said SRL for said file; and

transmitting, from said storage center to said end-user computer, said file identified by said SRL.

2. The method as set forth in claim 1, further comprising the steps of:

transmitting from said content server to said end-user computer an SRL further comprising an authentication certificate;

determining, at said storage center, using said authentication certificate, whether said request is valid; and

transmitting, from said storage center to said end-user computer, said file only if said request is valid.

3. The method as set forth in claim 1, further comprising the steps of:

transmitting to said end-user computer an SRL further comprising a time-out parameter; and

determining whether said request is valid through said time-out parameter.

4. The method as set forth in claim 1, further comprising the step of embedding said SRL into said content after receiving said request from an end-user computer for said content.

5. The method as set forth in claim 1, wherein:

the step of transmitting content comprises the step of transmitting hyper-text mark-up language ("HTML") content; and

the step of embedding said SRL into said content comprises the step of embedding said SRL into said HTML.

6. The method as set forth in claim 4, wherein the step of embedding said SRL into said content comprises the steps of:

storing at least one SRL for a file in an SRL file; and

extracting said SRL from said SRL file.

7. The method as set forth in claim 4, wherein the step of embedding said SRL into said content comprises the steps of:

coupling a local device comprising a cache to said content server;

storing at least one SRL for at least one file in said cache of said local device; and

extracting said SRL from said cache of said local device.

8. The method as set forth in claim 7, further comprising the step of: mounting said local device as a storage device for said content server for access to said SRLs.

9. The method as set forth in claim 1, further comprising the steps of:

storing at least one SRL for at least one file in an SRL file;

storing said file for access by a file system; and

organizing said SRL files in a file system, accessible to said content server, with a file structure substantially similar to said file structure for said files.

10. The method as set forth in claim 1, wherein:

the step of transmitting a request for said file from said end-user computer to a remote storage center comprises the step of transmitting a hyper-text transfer protocol ("HTTP") request; and

the step of transmitting said file from said storage center to said end-user computer comprises the step of transmitting said files using HTTP.

11. The method as set forth in claim 10, wherein the step of transmitting, from said storage center to said end-user computer, said file comprises the step of transferring a large media object.

12. A system comprising:

content server for receiving a request from an end-user computer for content, and for transmitting to said end-user computer, in response to said end-user request, said content comprising at least one storage resource locator ("SRL"), wherein said SRL comprises a unique file identifier to identify a file associated with said content;

storage center for receiving a request for said file from said end-user computer, including transmitting said SRL for said file, and for transmitting, from to said end-user computer, said file identified by said SRL.

13. The system as set forth in claim 12, wherein:

said SRL further comprises an authentication certificate; and

said storage center for determining whether said request is valid using said authentication certificate, and for and transmitting to said end-user computer said file only if said request is valid.

14. The system as set forth in claim 12, wherein:

said SRL further comprises a time-out parameter; and

said storage center for determining whether said request is valid through said time-out parameter.

15. The system as set forth in claim 12, wherein said content server further comprising processes for embedding said SRL into said content after receiving said request from an end-user computer for said content.

16. The system as set forth in claim 15, wherein:

said content comprises mark-up language ("HTML") content; and

said content server further comprising processes for embedding said SRL into said HTML.

17. The system as set forth in claim 15, wherein:

said SRL further comprising an SRL file; and

said content server further comprising processes for extracting said SRL from said SRL file.

18. The system as set forth in claim 12, further comprising a local device, coupled to said content server, that includes a cache for storing at least one SRL for at least one file in said cache of said local device, wherein said content server further comprising processes for extracting said SRL from said cache of said local device.

19. The system as set forth in claim 18, wherein said content server comprises processes for mounting said local device as a storage device to said SRLs.

20. The system as set forth in claim 19, further comprising a file system, accessible to said content server, including at least one SRL file for storing at least one SRL, wherein said file system comprising a file structure substantially similar to a file structure for said files.

21. A storage center comprising:

storage for storing a plurality of files;

storage control for receiving a request from an end-user computer, remote from said storage center, for at least one file, and for transmitting said file to said end-user computer, said request comprising at least one storage resource locator ("SRL") corresponding to said file, and wherein said SRL comprises a unique file identifier to identify said file associated with content that said end-user computer downloaded from a content server.

22. The storage center as set forth in claim 21, wherein:

said SRL further comprises an authentication certificate; and

said storage center for determining whether said request is valid using said authentication certificate, and for transmitting to said end-user computer said file only if said request is valid.

23. The storage center as set forth in claim 21, wherein:

said SRL further comprises a time-out parameter; and

said storage center for determining whether said request is valid through said time-out parameter.

5

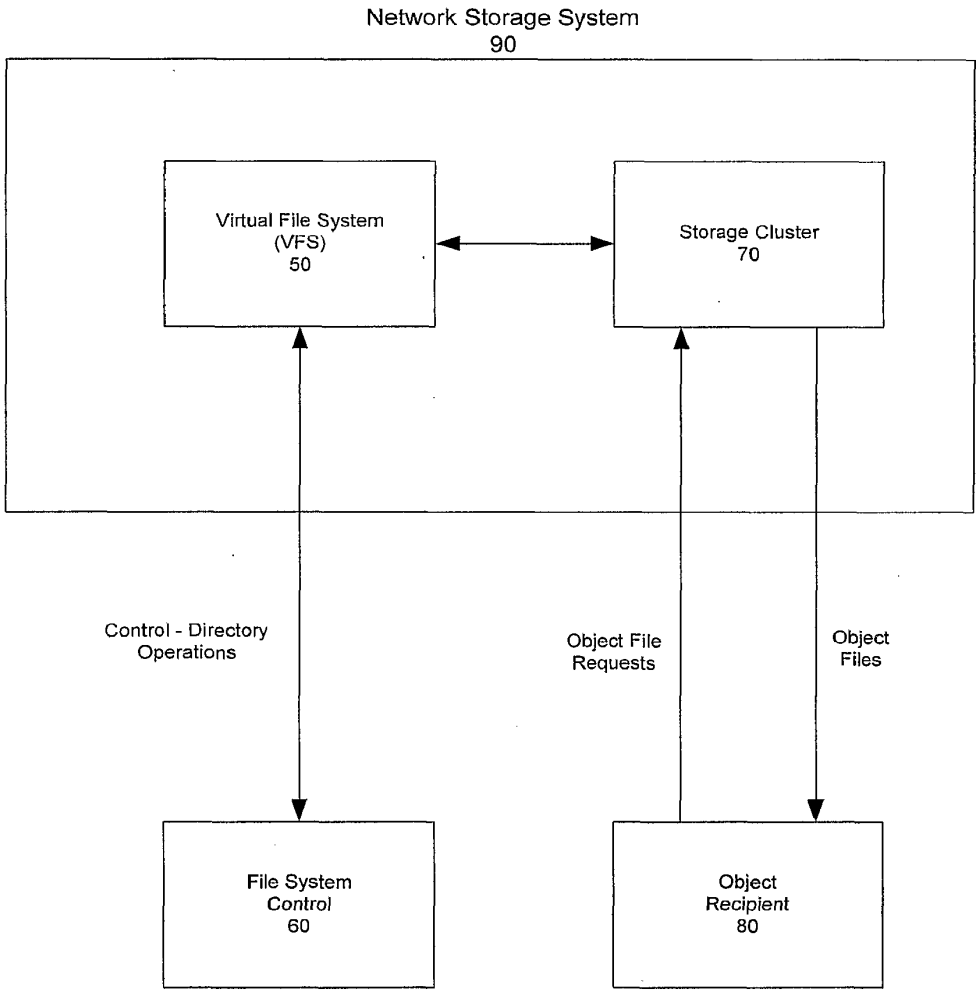

Network Storage System
90
Virtual File System
(VFS)
50
Storage Cluster
70
Control - Directory
Operations
Object File
Requests
Object
Files
File System
Control
60
Object
Recipient
80

Figure 1

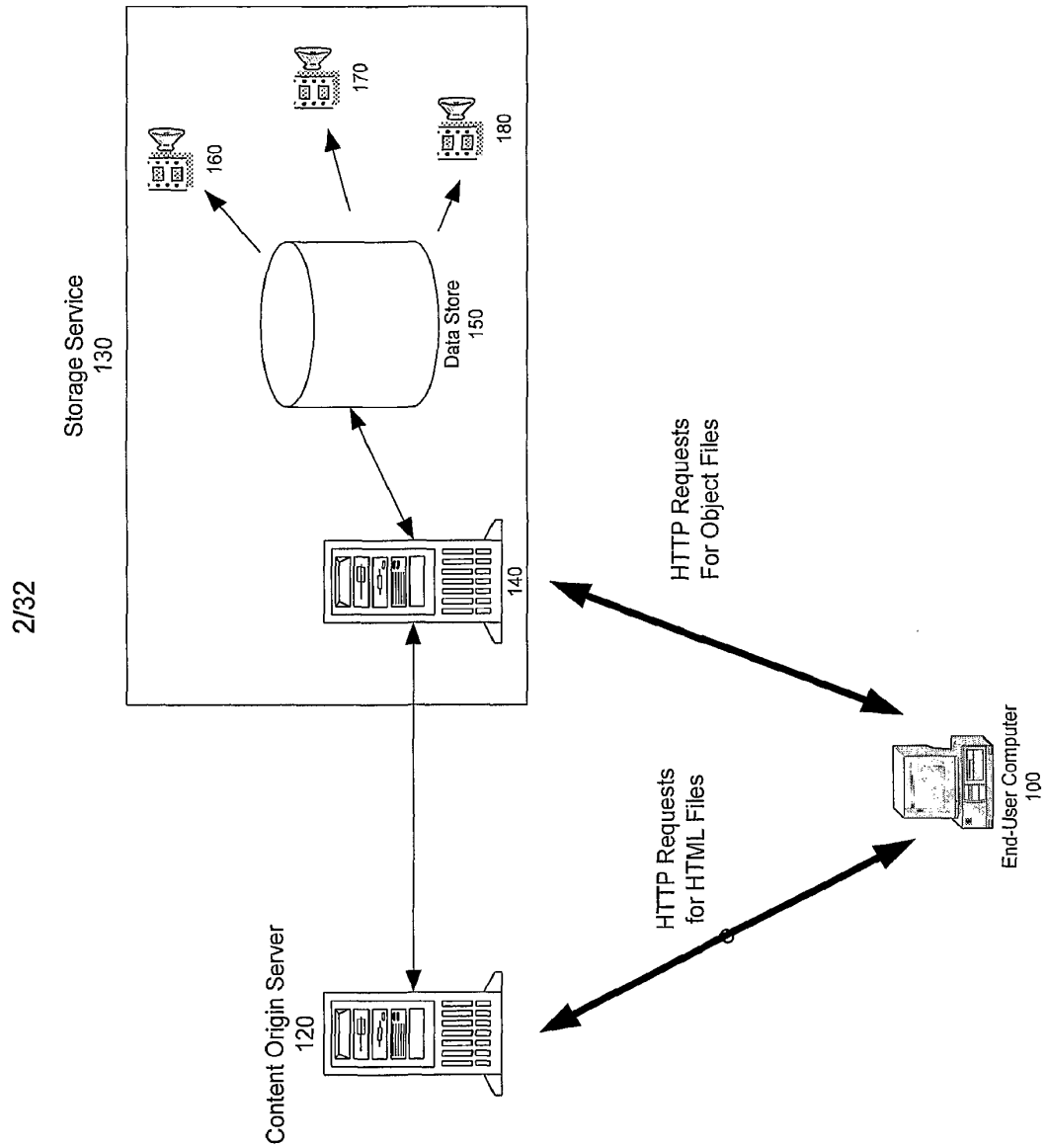

Storage Service
130
160
170
180
Data Store
150
140
HTTP Requests
For Object Files
HTTP Requests
for HTML Files
End-User Computer
100
Content Origin Server
120

Figure 2

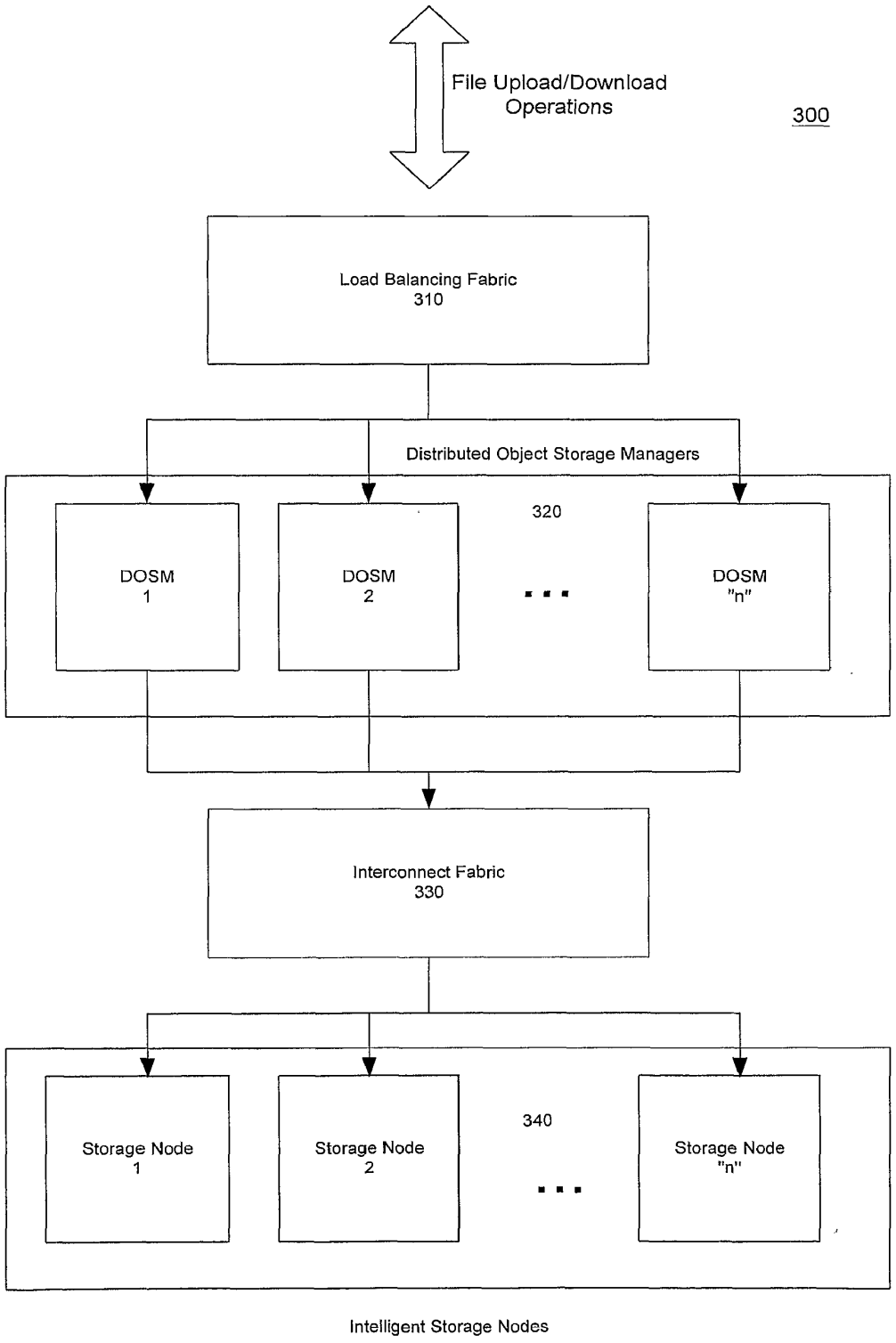

File Upload/Download Operations
300
Load Balancing Fabric 310
Distributed Object Storage Managers
320
DOSM 1
DOSM 2
DOSM "n"
Interconnect Fabric 330
340
Storage Node 1
Storage Node 2
Storage Node "n"
Intelligent Storage Nodes

Figure 3

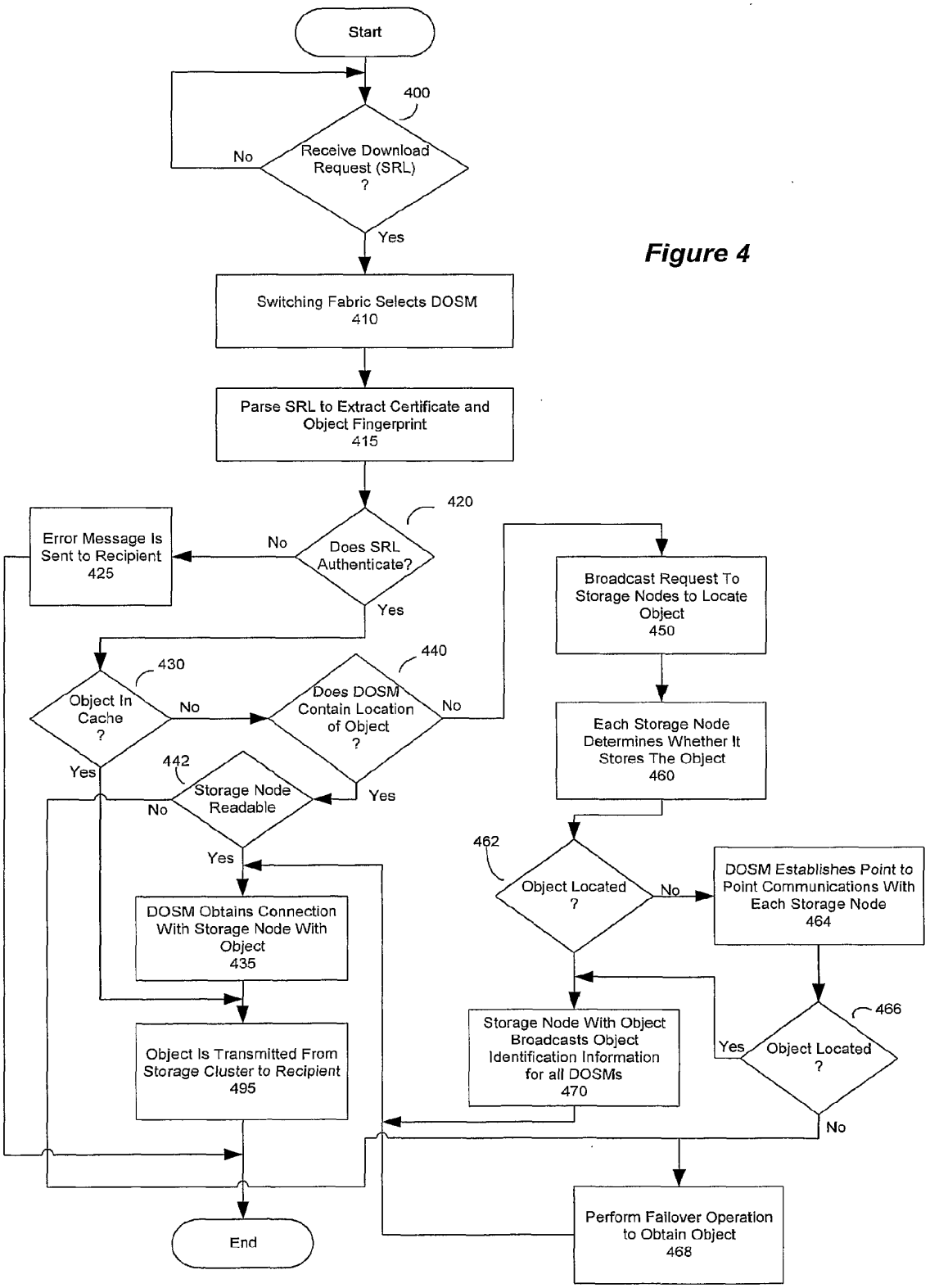

Start
400
Receive Download Request (SRL) ?
No
Yes
Switching Fabric Selects DOSM 410
Parse SRL to Extract Certificate and Object Fingerprint 415
420
Does SRL Authenticate?
No
Error Message Is Sent to Recipient 425
Yes
430
Object In Cache ?
No
Yes
440
Does DOSM Contain Location of Object ?
No
Yes
442
Storage Node Readable
No
Yes
DOSM Obtains Connection With Storage Node With Object 435
Object Is Transmitted From Storage Cluster to Recipient 495
End
Broadcast Request To Storage Nodes to Locate Object 450
Each Storage Node Determines Whether It Stores The Object 460
462
Object Located ?
No
DOSM Establishes Point to Point Communications With Each Storage Node 464
Storage Node With Object Broadcasts Object Identification Information for all DOSMs 470
466
Yes
Object Located ?
No
Perform Failover Operation to Obtain Object 468

Figure 4

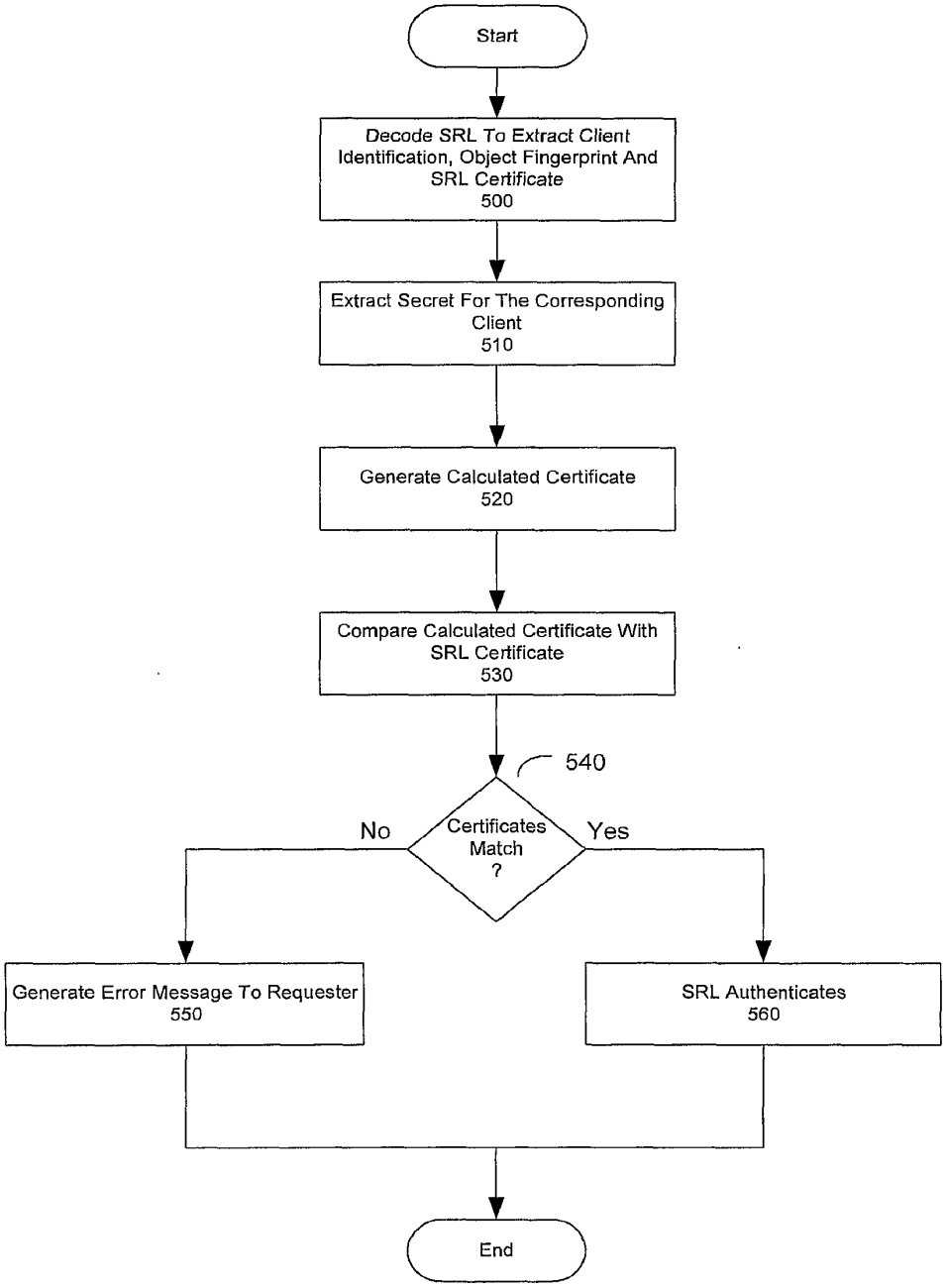

Start
Decode SRL To Extract Client Identification, Object Fingerprint And SRL Certificate
500
Extract Secret For The Corresponding Client
510
Generate Calculated Certificate
520
Compare Calculated Certificate With SRL Certificate
530
540
Certificates Match ?
No
Yes
Generate Error Message To Requester
550
SRL Authenticates
560
End

Figure 5

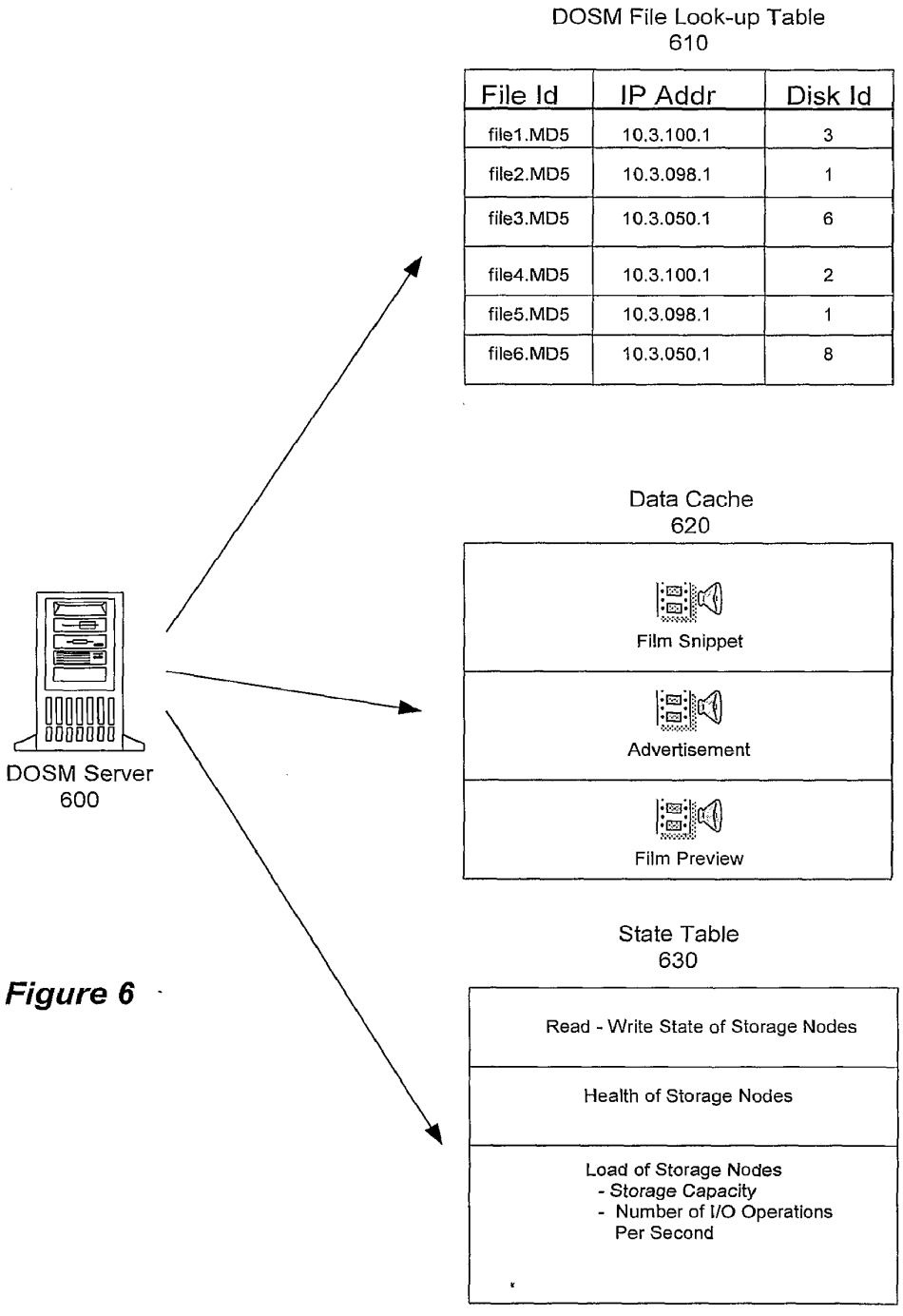

DOSM File Look-up Table
610
File Id
IP Addr
Disk Id
file1.MD5
10.3.100.1
3
file2.MD5
10.3.098.1
1
file3.MD5
10.3.050.1
6
file4.MD5
10.3.100.1
2
file5.MD5
10.3.098.1
1
file6.MD5
10.3.050.1
8
Data Cache
620
Film Snippet
Advertisement
Film Preview
DOSM Server
600
State Table
630
Read - Write State of Storage Nodes
Health of Storage Nodes
Load of Storage Nodes
- Storage Capacity
- Number of I/O Operations Per Second

Figure 6

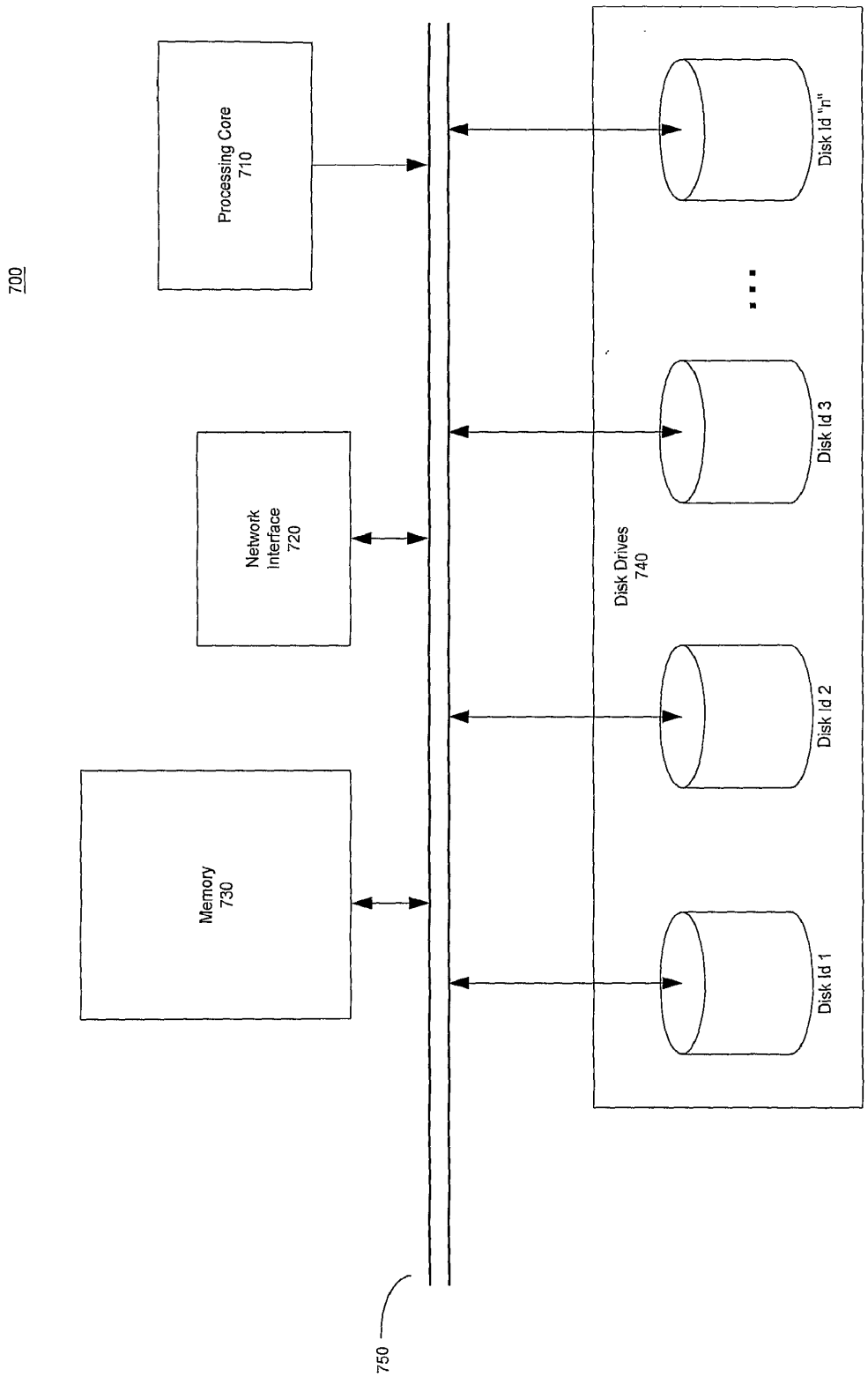

700
Processing Core
710
Network
Interface
720
Memory
730
750
Disk Drives
740
Disk Id 1
Disk Id 2
Disk Id 3
Disk Id "n"

Figure 7

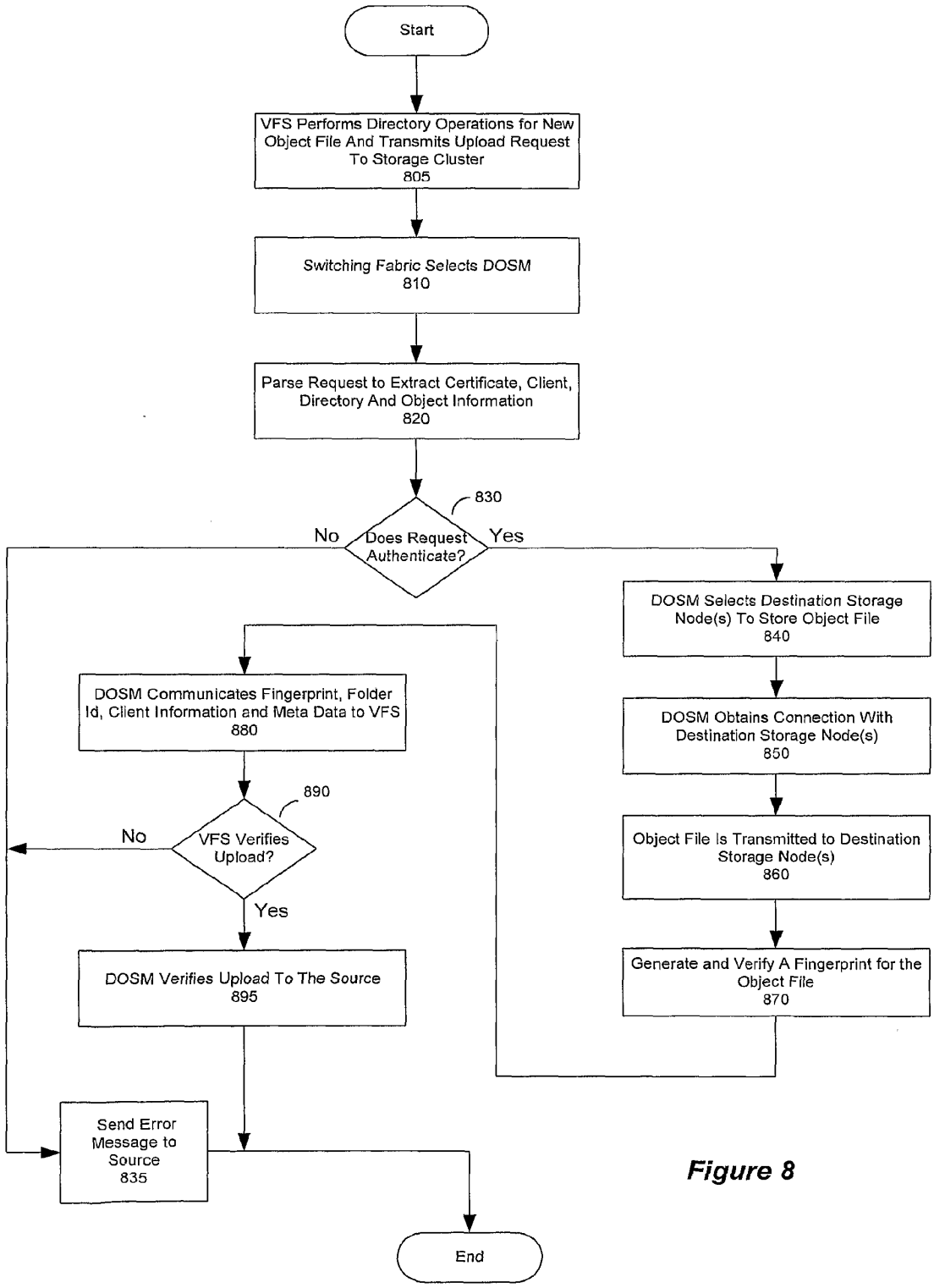

Start
VFS Performs Directory Operations for New Object File And Transmits Upload Request To Storage Cluster
805
Switching Fabric Selects DOSM
810
Parse Request to Extract Certificate, Client, Directory And Object Information
820
830
Does Request Authenticate?
No
Yes
DOSM Selects Destination Storage Node(s) To Store Object File
840
DOSM Obtains Connection With Destination Storage Node(s)
850
Object File Is Transmitted to Destination Storage Node(s)
860
Generate and Verify A Fingerprint for the Object File
870
DOSM Communicates Fingerprint, Folder Id, Client Information and Meta Data to VFS
880
890
VFS Verifies Upload?
No
Yes
DOSM Verifies Upload To The Source
895
Send Error Message to Source
835
End

Figure 8

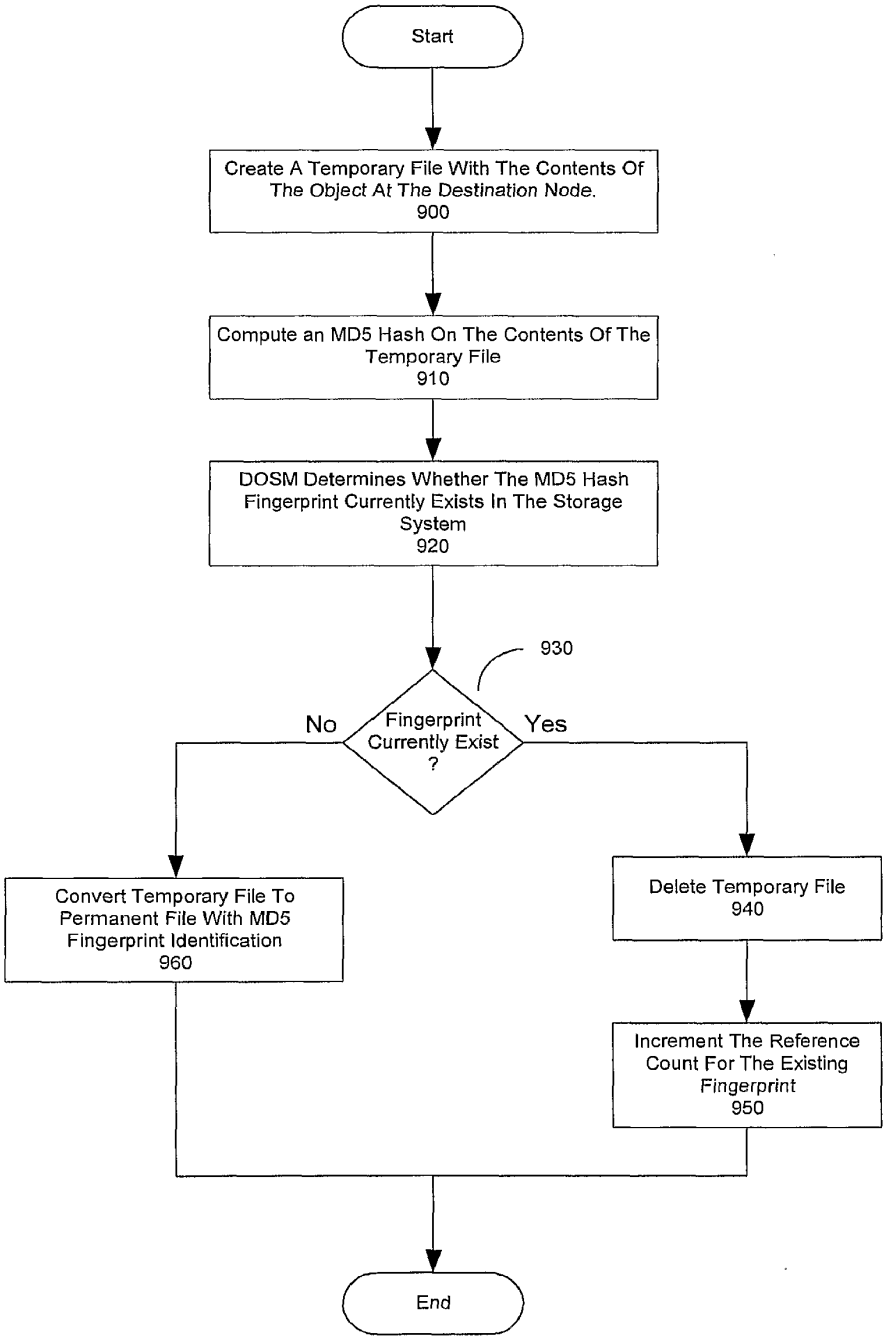
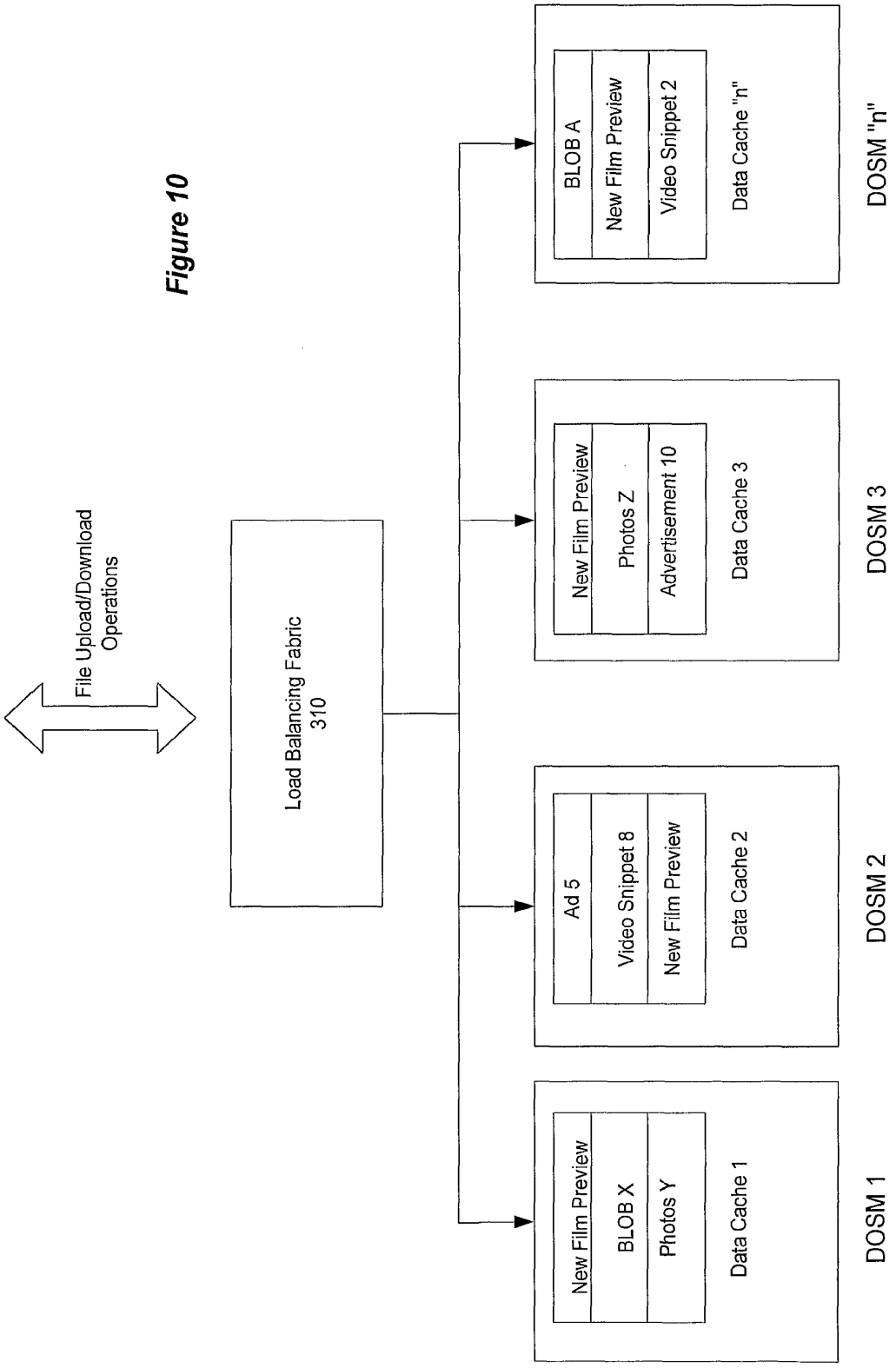

Start
Create A Temporary File With The Contents Of The Object At The Destination Node.
900
Compute an MD5 Hash On The Contents Of The Temporary File
910
DOSM Determines Whether The MD5 Hash Fingerprint Currently Exists In The Storage System
920
930
Fingerprint Currently Exist ?
No
Yes
Convert Temporary File To Permanent File With MD5 Fingerprint Identification
960
Delete Temporary File
940
Increment The Reference Count For The Existing Fingerprint
950
End

Figure 9

Figure 10


File Upload/Download Operations
Load Balancing Fabric 310
DOSM 1
Data Cache 1
New Film Preview
BLOB X
Photos Y
DOSM 2
Data Cache 2
Ad 5
Video Snippet 8
New Film Preview
DOSM 3
Data Cache 3
New Film Preview
Photos Z
Advertisement 10
DOSM "n"
Data Cache "n"
BLOB A
New Film Preview
Video Snippet 2

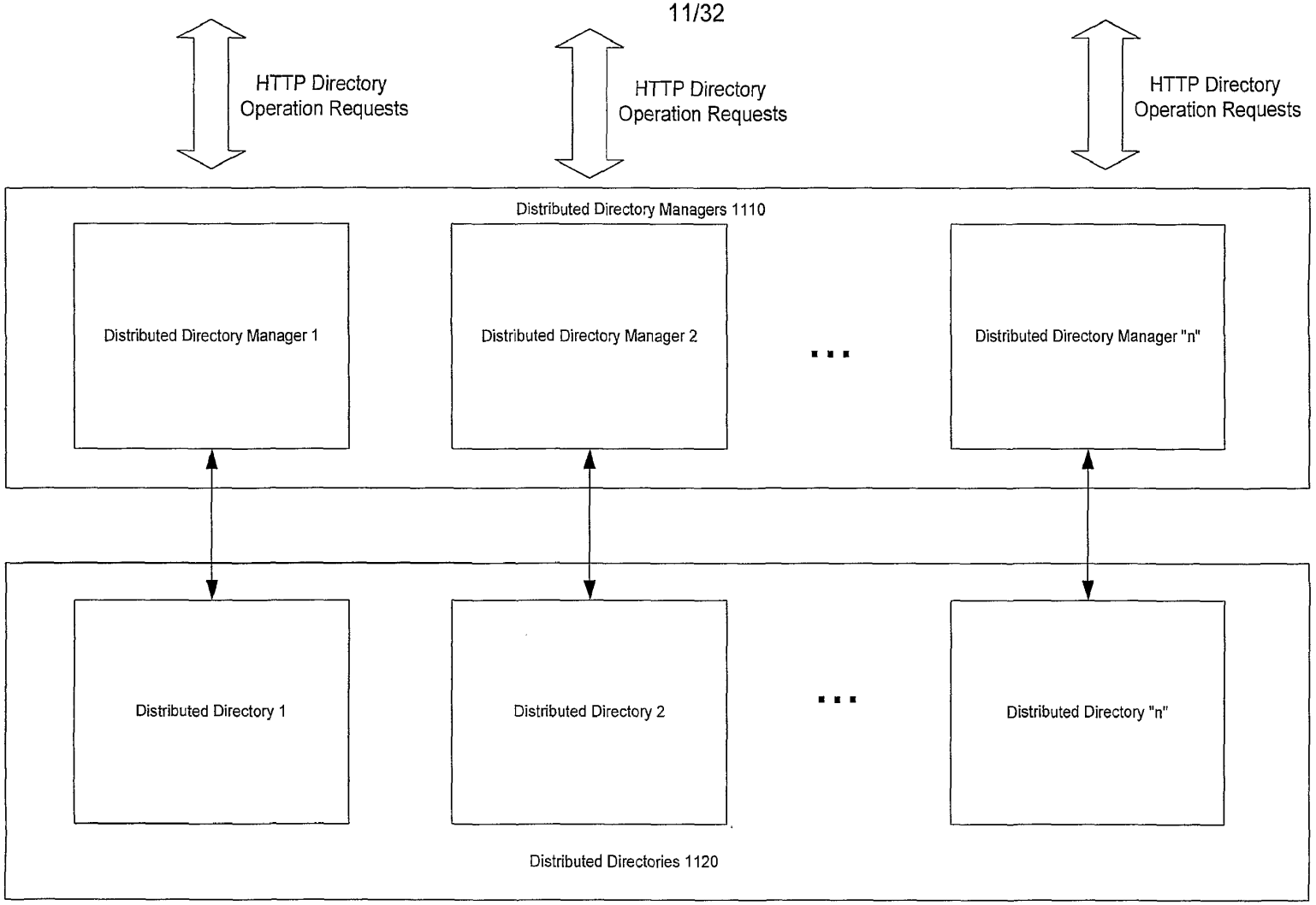


Figure 11

1100

Customer Table

	Customer Name	Customer Reserved Fields
	Customer A	[Customer stores data ...]
	Customer B	[Customer stores data ...]
	Customer C	[Customer stores data ...]
	Customer D	[Customer stores data ...]

1200

Folder Table

Customer Id	Folder Id	Folder Parent Id	Metadata
3	2	-	[Reserved]
3	100	2	[Reserved]
3	251	2	[Reserved]
3	166	251	[Reserved]

1210

File Table

Customer Id	File Handle	Folder Id	Folder Parent Id	Metadata
3	52.MD5	100	2	[Reserved]
3	55.MD5	100	2	[Reserved]
3	99.MD5	166	251	[Reserved]
3	67.MD5	166	251	[Reserved]

1220

Figure 12

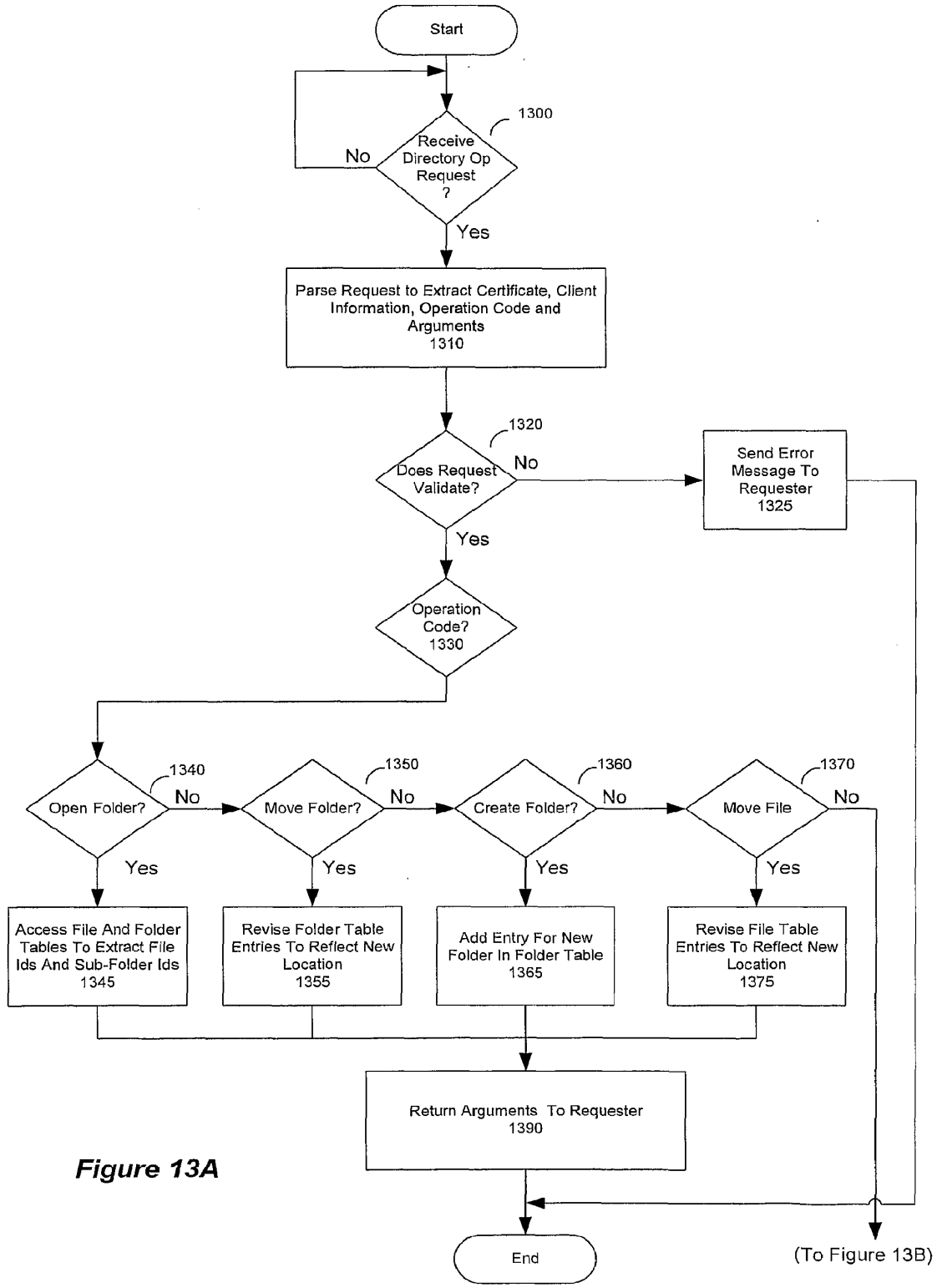

Start
1300
Receive Directory Op Request ?
No
Yes
Parse Request to Extract Certificate, Client Information, Operation Code and Arguments
1310
1320
Does Request Validate?
No
Send Error Message To Requester
1325
Yes
Operation Code?
1330
1340
Open Folder?
No
1350
Move Folder?
No
1360
Create Folder?
No
1370
Move File
No
Yes
Yes
Yes
Yes
Access File And Folder Tables To Extract File Ids And Sub-Folder Ids
1345
Revise Folder Table Entries To Reflect New Location
1355
Add Entry For New Folder In Folder Table
1365
Revise File Table Entries To Reflect New Location
1375
Return Arguments To Requester
1390
End
(To Figure 13B)

Figure 13A

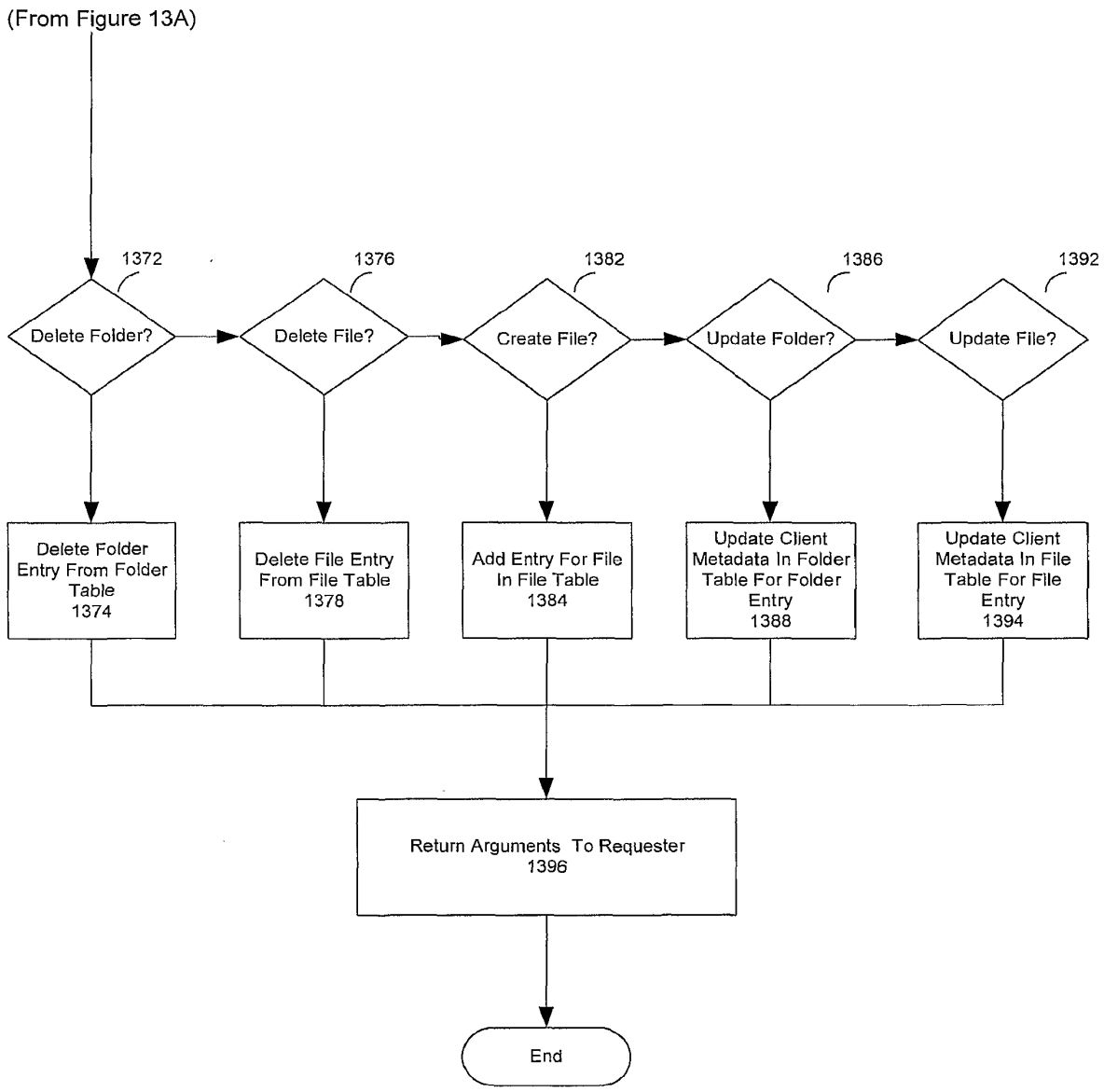

(From Figure 13A)
1372
Delete Folder?
1376
Delete File?
1382
Create File?
1386
Update Folder?
1392
Update File?
Delete Folder Entry From Folder Table 1374
Delete File Entry From File Table 1378
Add Entry For File In File Table 1384
Update Client Metadata In Folder Table For Folder Entry 1388
Update Client Metadata In File Table For File Entry 1394
Return Arguments To Requester 1396
End

Figure 13B

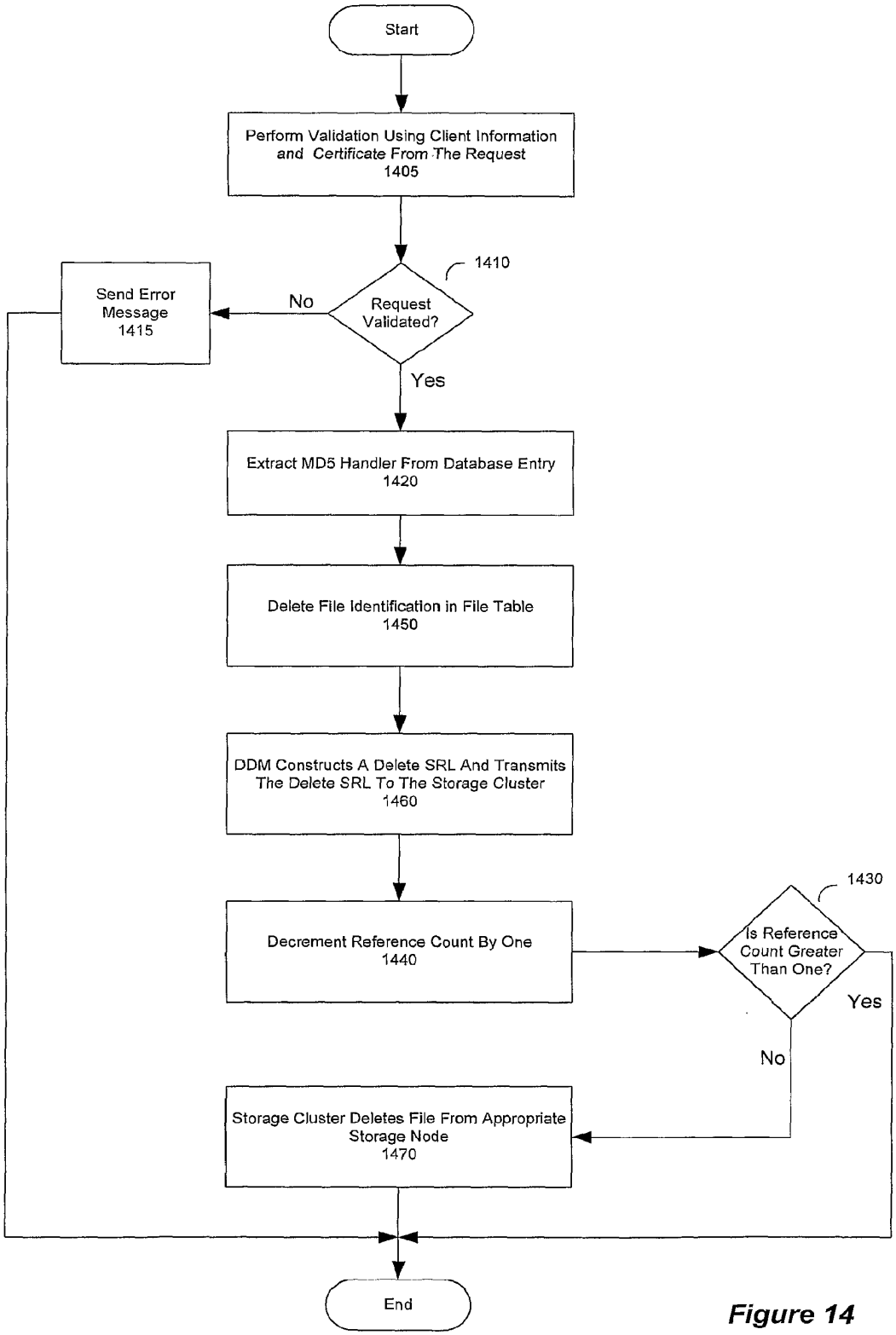

Start
Perform Validation Using Client Information and Certificate From The Request
1405
1410
Request Validated?
No
Send Error Message
1415
Yes
Extract MD5 Handler From Database Entry
1420
Delete File Identification in File Table
1450
DDM Constructs A Delete SRL And Transmits The Delete SRL To The Storage Cluster
1460
Decrement Reference Count By One
1440
1430
Is Reference Count Greater Than One?
Yes
No
Storage Cluster Deletes File From Appropriate Storage Node
1470
End

Figure 14

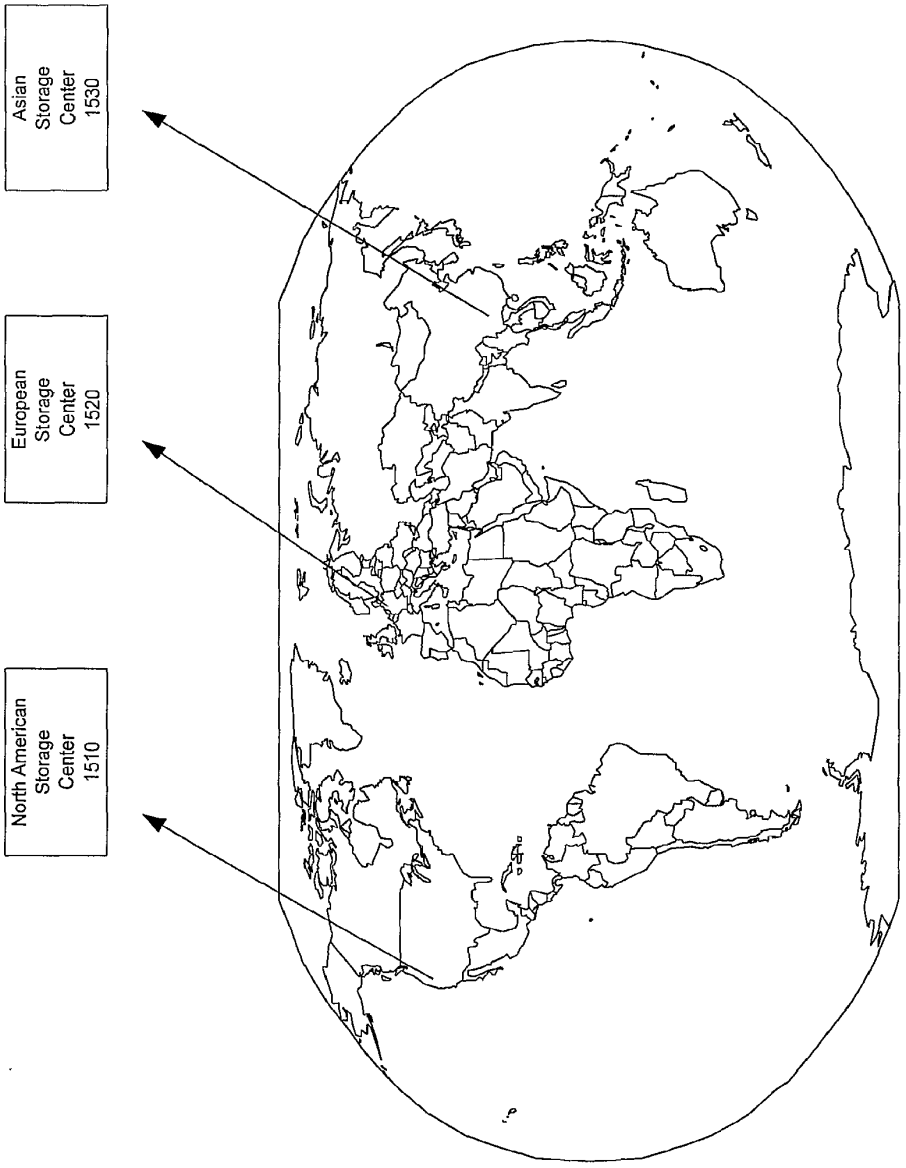

Asian Storage Center 1530
European Storage Center 1520
North American Storage Center 1510

Figure 15

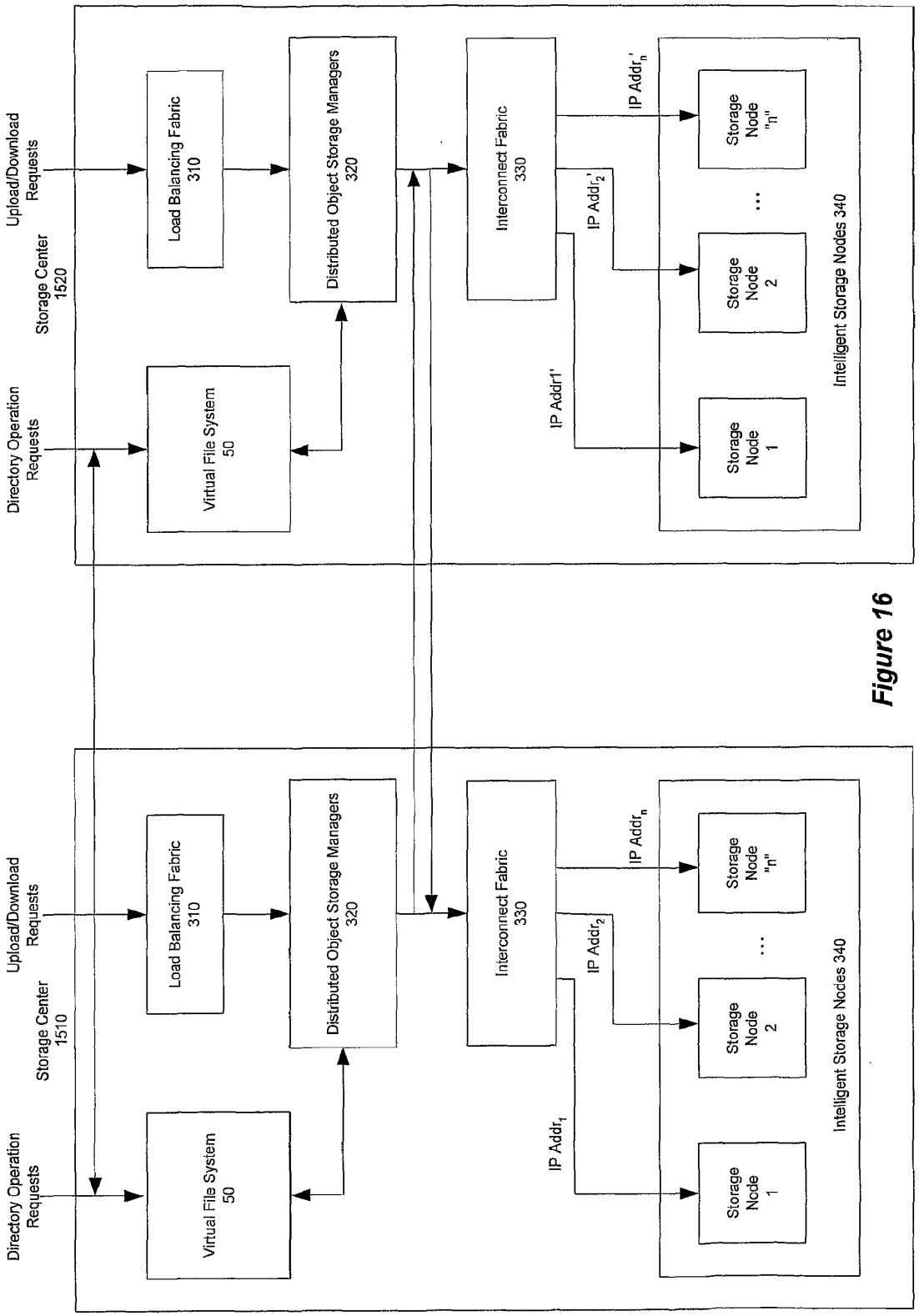

Storage Center 1520
Upload/Download Requests
Directory Operation Requests
Load Balancing Fabric 310
Virtual File System 50
Distributed Object Storage Managers 320
Interconnect Fabric 330
IP Addr1'
IP Addr2'
IP Addrn'
Storage Node 1
Storage Node 2
Storage Node "n"
Intelligent Storage Nodes 340
Storage Center 1510
Upload/Download Requests
Directory Operation Requests
Load Balancing Fabric 310
Virtual File System 50
Distributed Object Storage Managers 320
Interconnect Fabric 330
IP Addr1
IP Addr2
IP Addrn
Storage Node 1
Storage Node 2
Storage Node "n"
Intelligent Storage Nodes 340

Figure 16

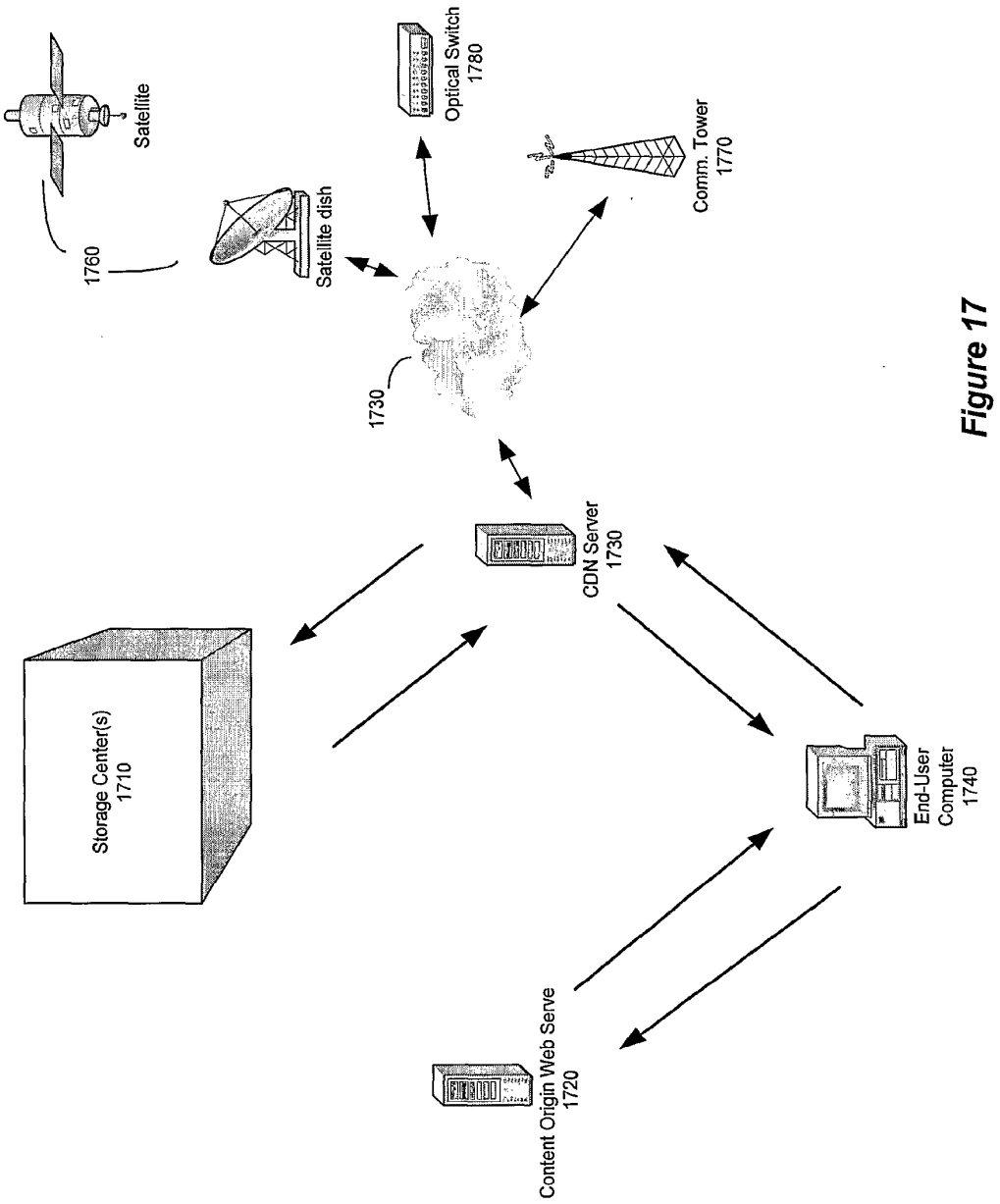

Satellite
1760
Satellite dish
Optical Switch
1780
Comm. Tower
1770
1730
CDN Server
1730
Storage Center(s)
1710
End-User
Computer
1740
Content Origin Web Serve
1720

Figure 17

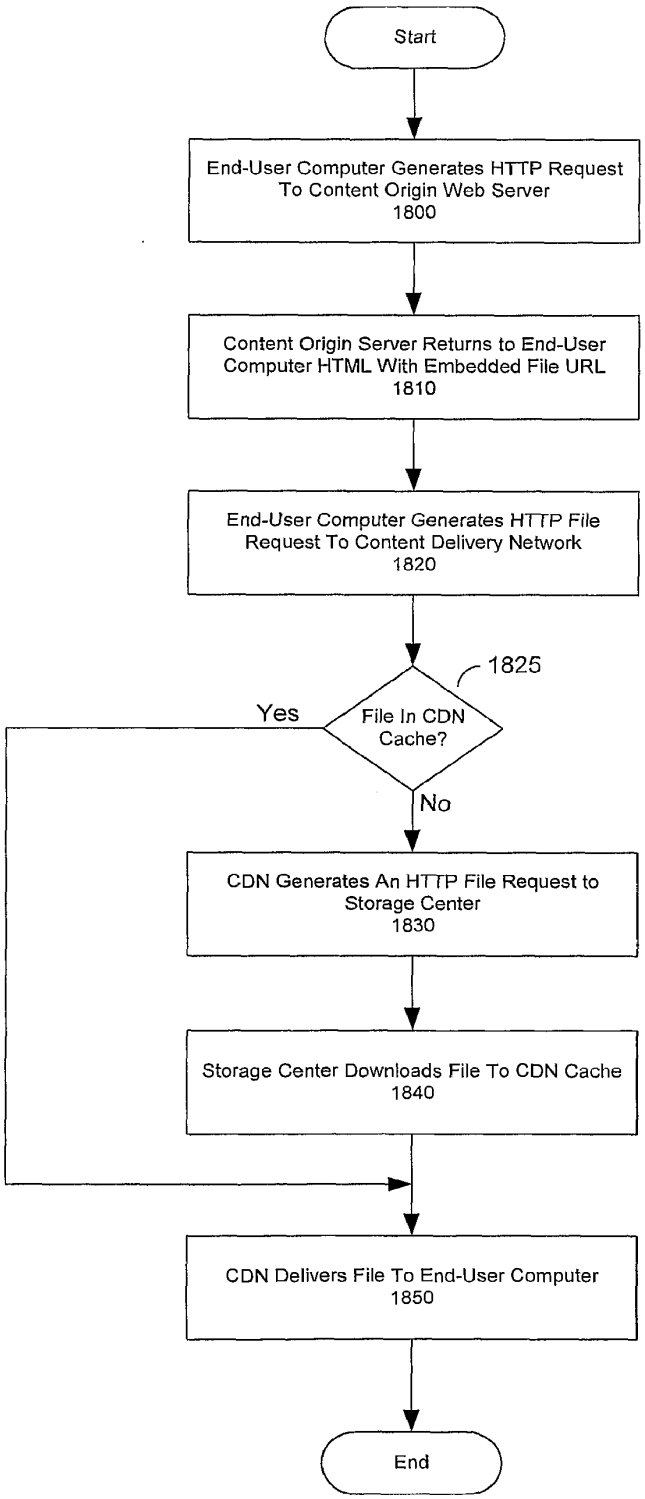

Start
End-User Computer Generates HTTP Request To Content Origin Web Server 1800
Content Origin Server Returns to End-User Computer HTML With Embedded File URL 1810
End-User Computer Generates HTTP File Request To Content Delivery Network 1820
1825
File In CDN Cache?
Yes
No
CDN Generates An HTTP File Request to Storage Center 1830
Storage Center Downloads File To CDN Cache 1840
CDN Delivers File To End-User Computer 1850
End

Figure 18

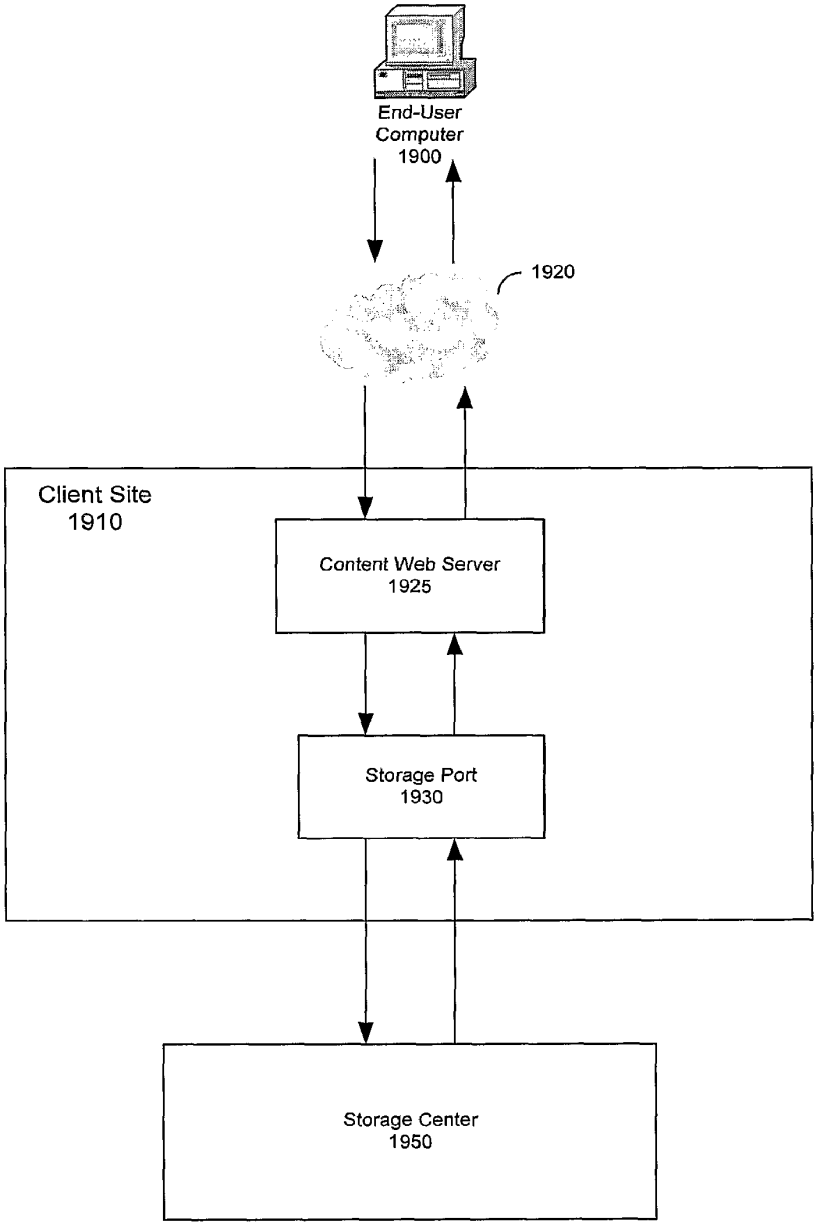

End-User
Computer
1900
1920
Client Site
1910
Content Web Server
1925
Storage Port
1930
Storage Center
1950

Figure 19

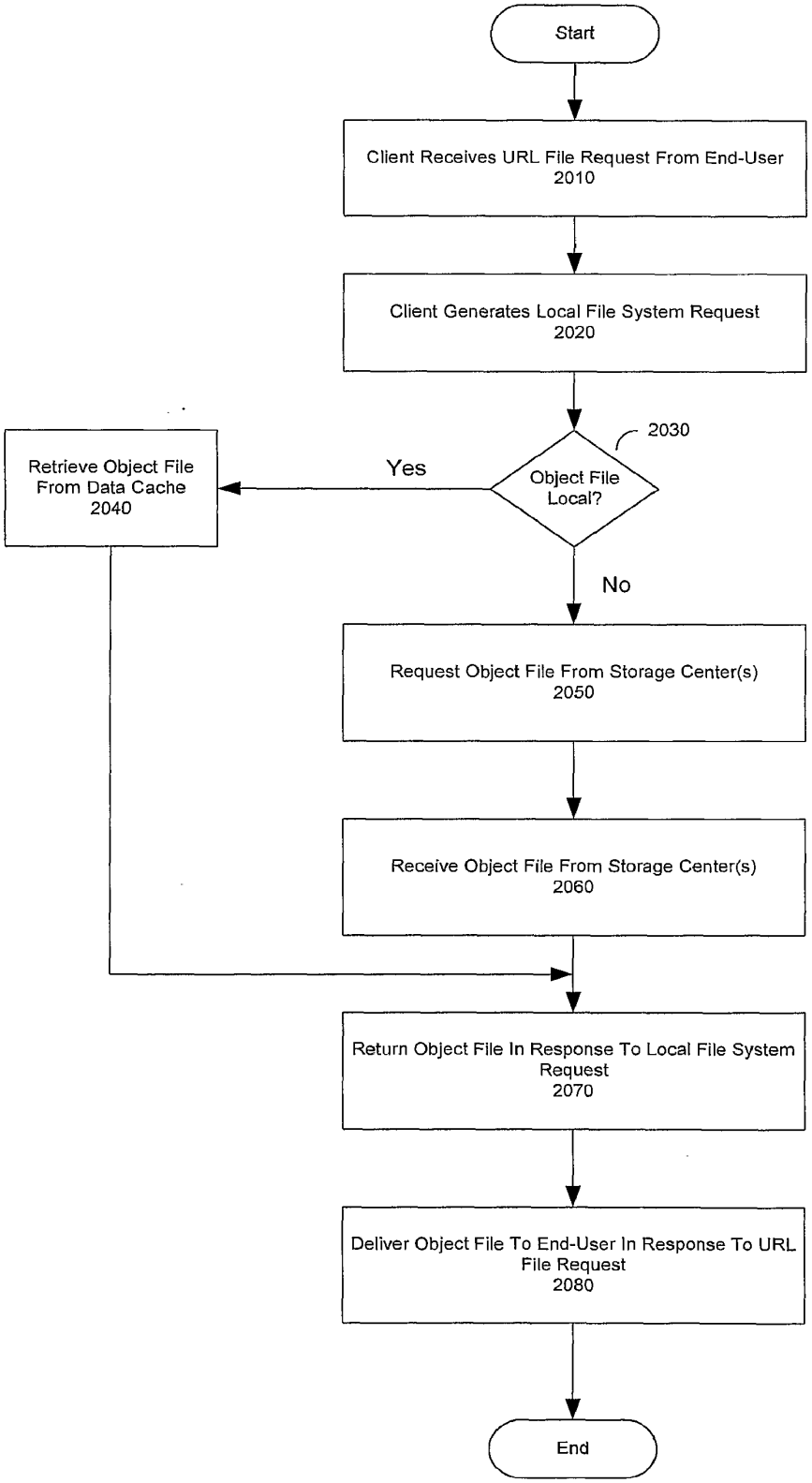

Start
Client Receives URL File Request From End-User
2010
Client Generates Local File System Request
2020
2030
Object File Local?
Yes
Retrieve Object File From Data Cache
2040
No
Request Object File From Storage Center(s)
2050
Receive Object File From Storage Center(s)
2060
Return Object File In Response To Local File System Request
2070
Deliver Object File To End-User In Response To URL File Request
2080
End

Figure 20

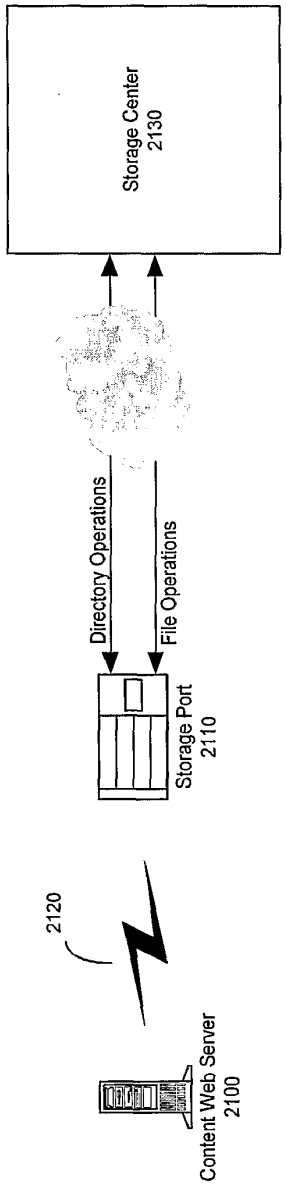


Figure 21a

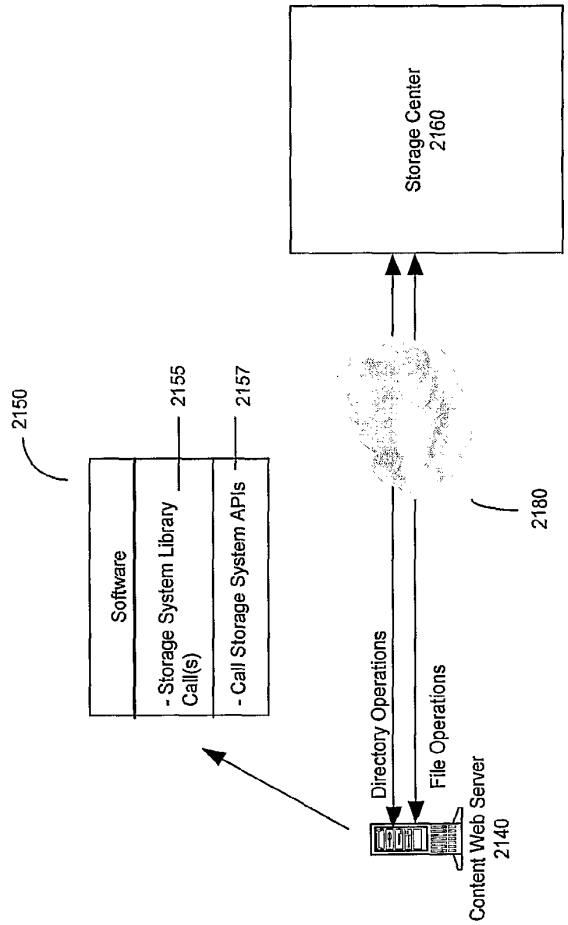


Figure 21b

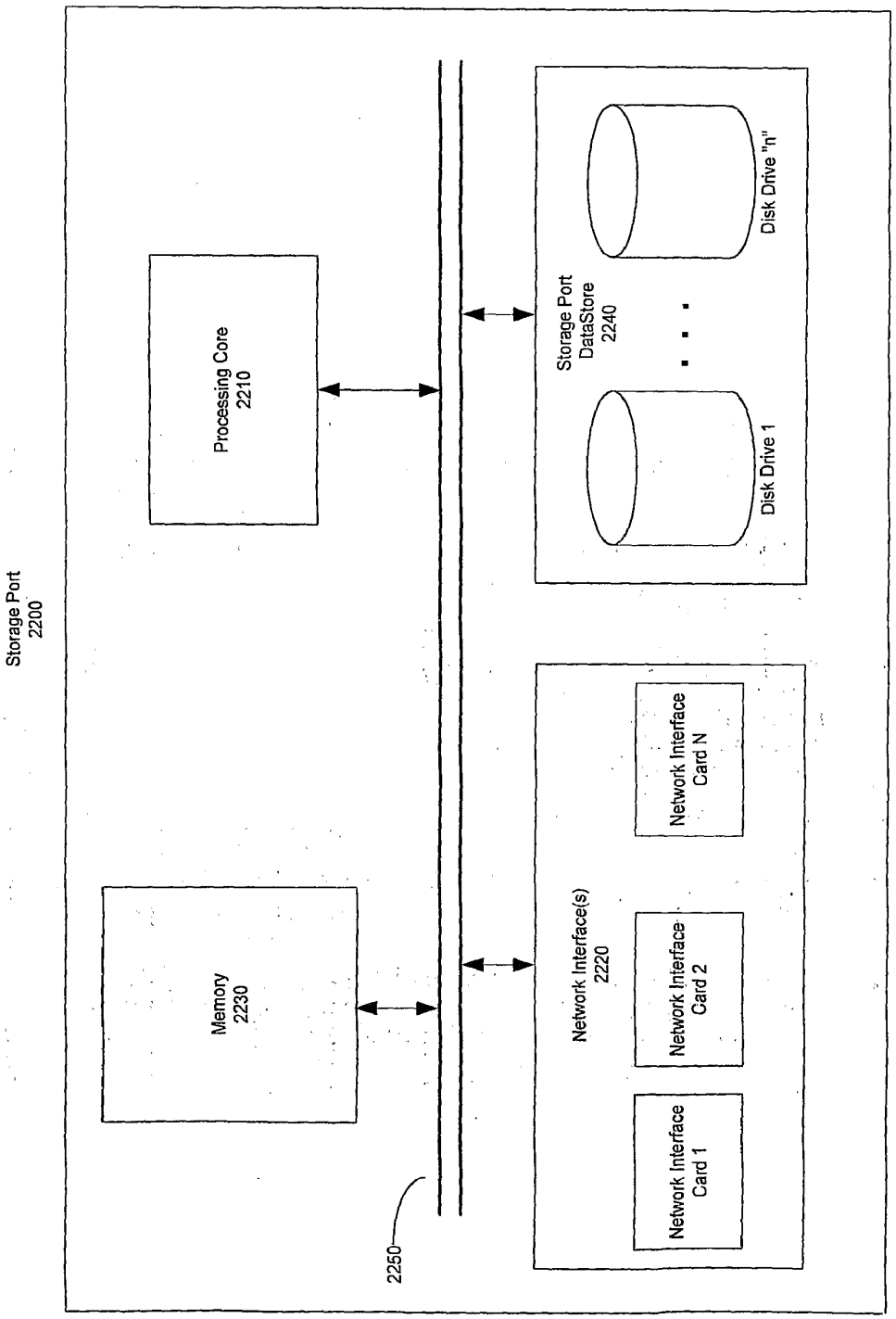

Storage Port
2200
Processing Core
2210
Memory
2230
2250
Network Interface(s)
2220
Network Interface
Card 1
Network Interface
Card 2
Network Interface
Card N
Storage Port
DataStore
2240
Disk Drive 1
Disk Drive "n"

Figure 22

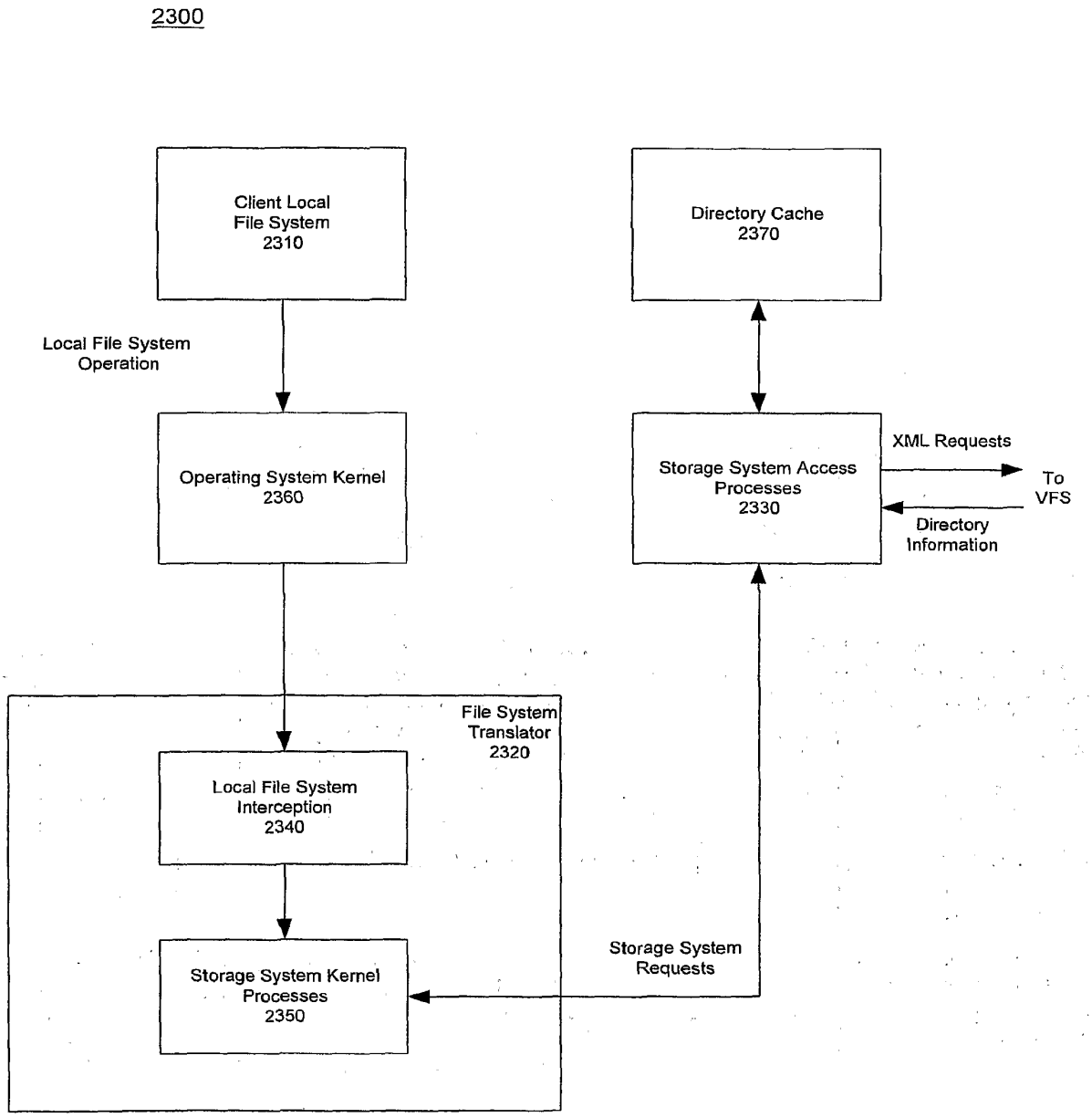

2300
Client Local File System 2310
Directory Cache 2370
Local File System Operation
Operating System Kernel 2360
Storage System Access Processes 2330
XML Requests
To VFS
Directory Information
File System Translator 2320
Local File System Interception 2340
Storage System Kernel Processes 2350
Storage System Requests

Figure 23

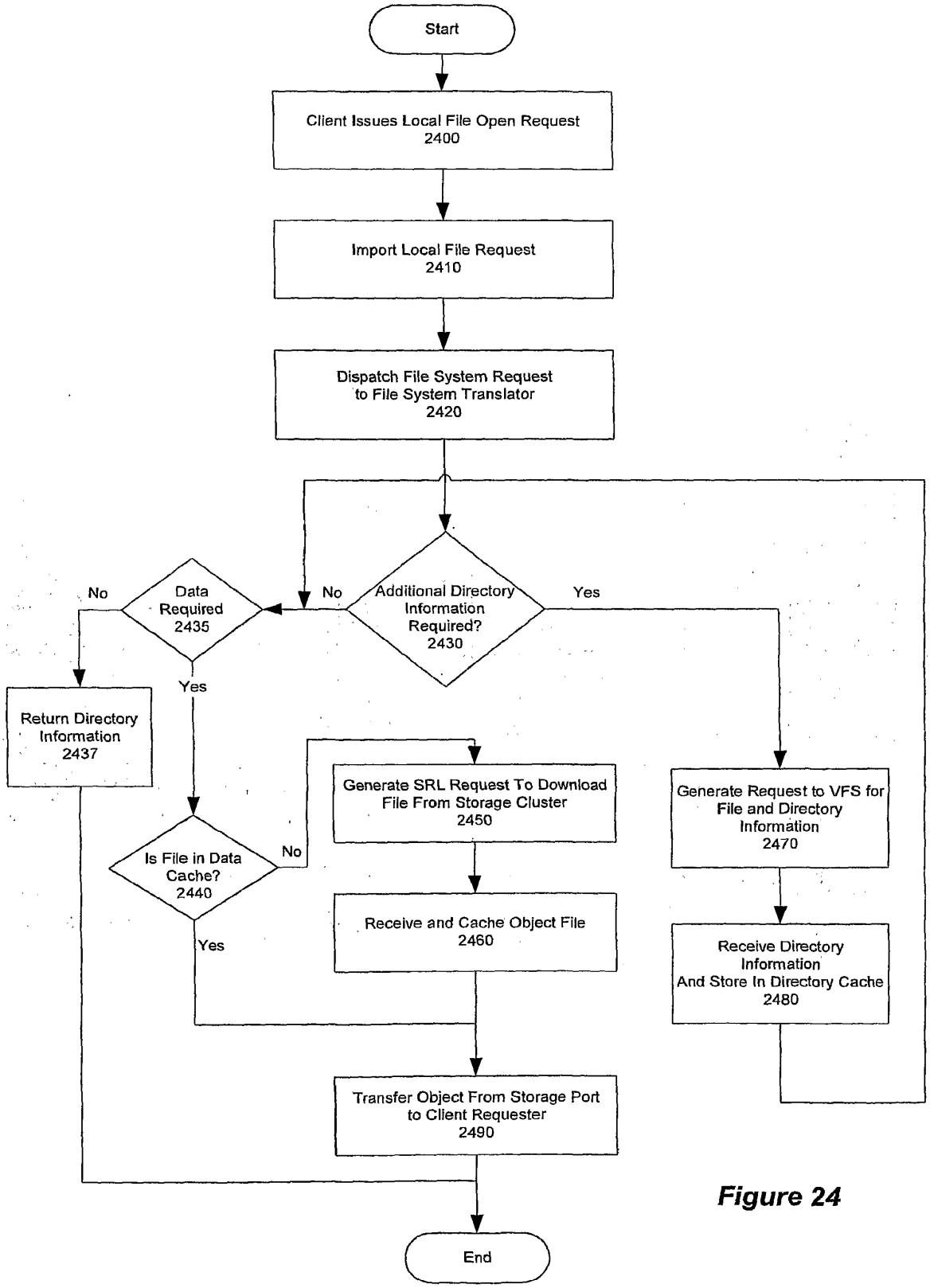

Start
Client Issues Local File Open Request
2400
Import Local File Request
2410
Dispatch File System Request
to File System Translator
2420
Additional Directory
Information
Required?
2430
No
Yes
Data
Required
2435
No
Yes
Return Directory
Information
2437
Is File in Data
Cache?
2440
No
Yes
Generate SRL Request To Download
File From Storage Cluster
2450
Receive and Cache Object File
2460
Generate Request to VFS for
File and Directory
Information
2470
Receive Directory
Information
And Store In Directory Cache
2480
Transfer Object From Storage Port
to Client Requester
2490
End

Figure 24

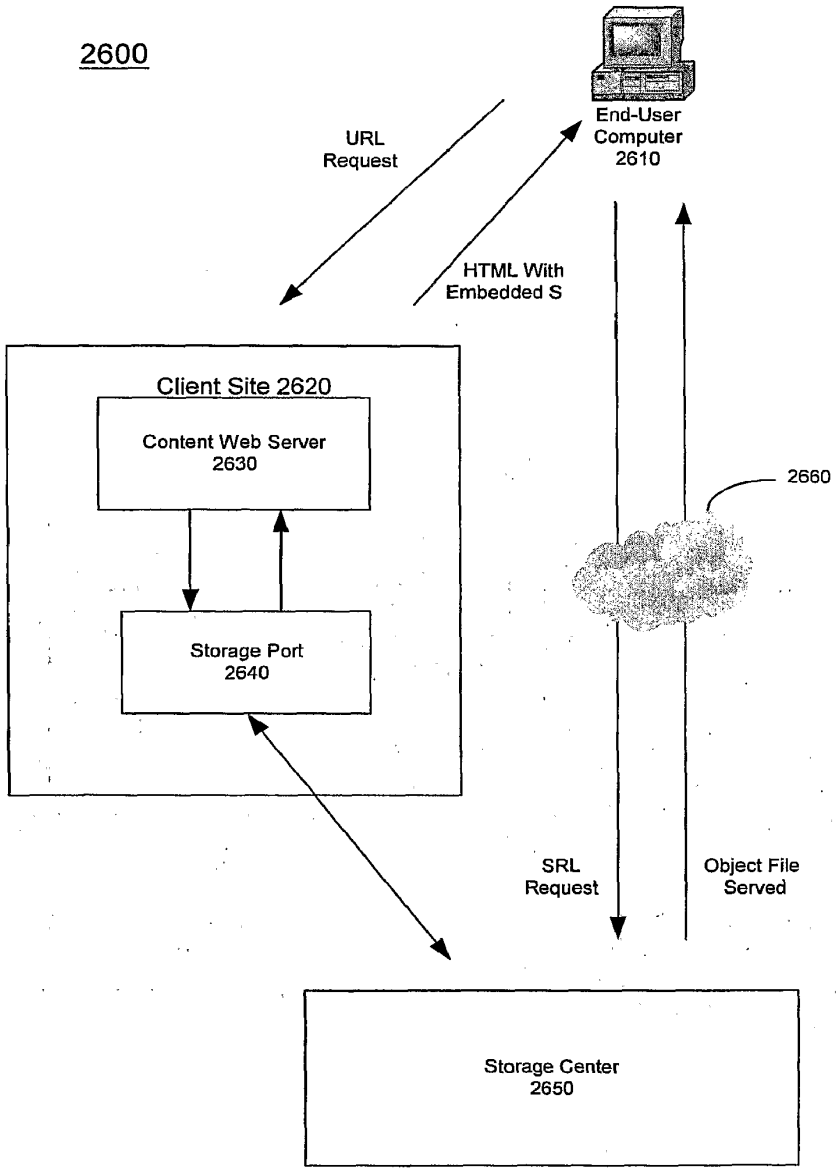

2600
End-User Computer 2610
URL Request
HTML With Embedded S
Client Site 2620
Content Web Server 2630
Storage Port 2640
2660
SRL Request
Object File Served
Storage Center 2650

Figure 25

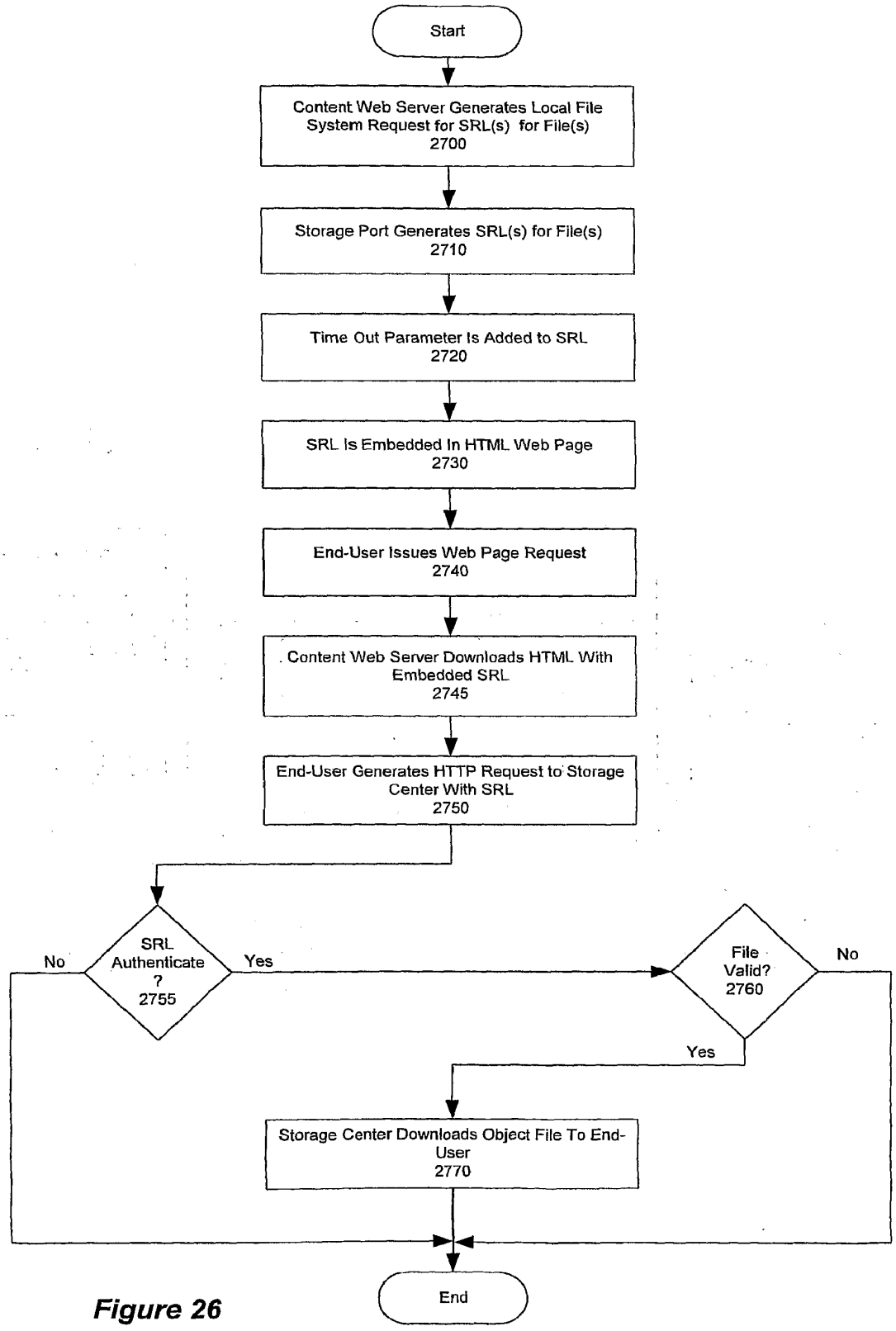

Start
Content Web Server Generates Local File System Request for SRL(s) for File(s) 2700
Storage Port Generates SRL(s) for File(s) 2710
Time Out Parameter Is Added to SRL 2720
SRL Is Embedded In HTML Web Page 2730
End-User Issues Web Page Request 2740
Content Web Server Downloads HTML With Embedded SRL 2745
End-User Generates HTTP Request to Storage Center With SRL 2750
SRL Authenticate ? 2755
No
Yes
File Valid? 2760
No
Yes
Storage Center Downloads Object File To End-User 2770
End

Figure 26

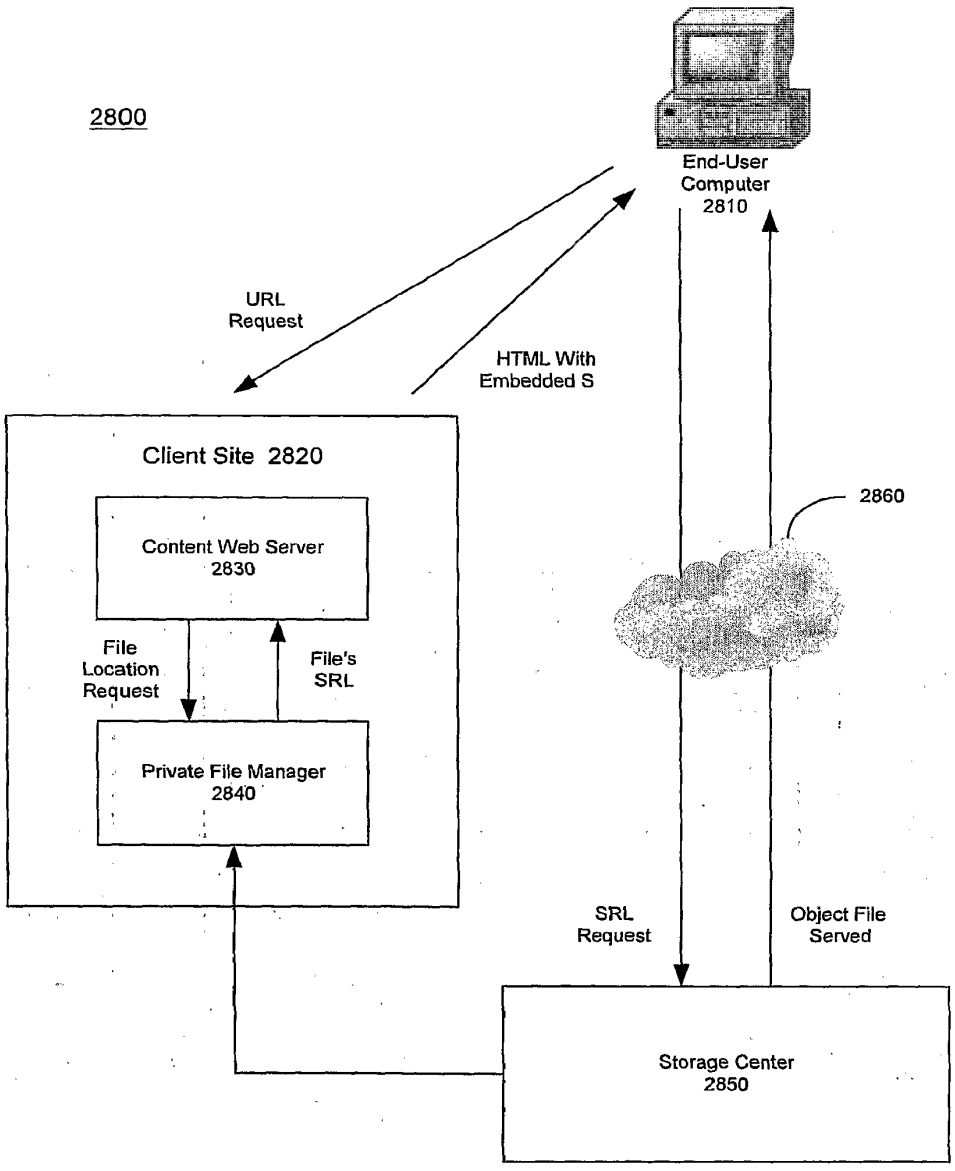

2800
End-User
Computer
2810
URL
Request
HTML With
Embedded S
Client Site 2820
Content Web Server
2830
File
Location
Request
File's
SRL
Private File Manager
2840
2860
SRL
Request
Object File
Served
Storage Center
2850

Figure 27

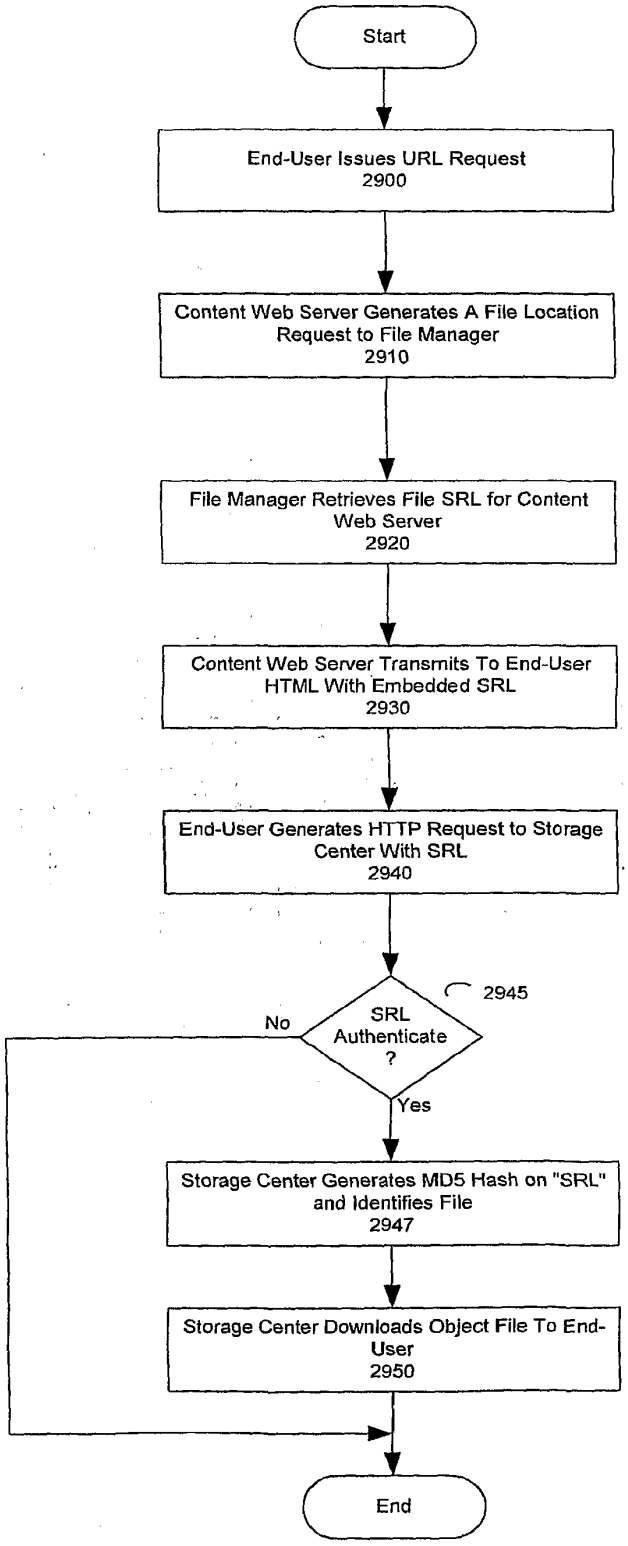

Start
End-User Issues URL Request
2900
Content Web Server Generates A File Location Request to File Manager
2910
File Manager Retrieves File SRL for Content Web Server
2920
Content Web Server Transmits To End-User HTML With Embedded SRL
2930
End-User Generates HTTP Request to Storage Center With SRL
2940
2945
SRL Authenticate ?
No
Yes
Storage Center Generates MD5 Hash on "SRL" and Identifies File
2947
Storage Center Downloads Object File To End-User
2950
End

Figure 28

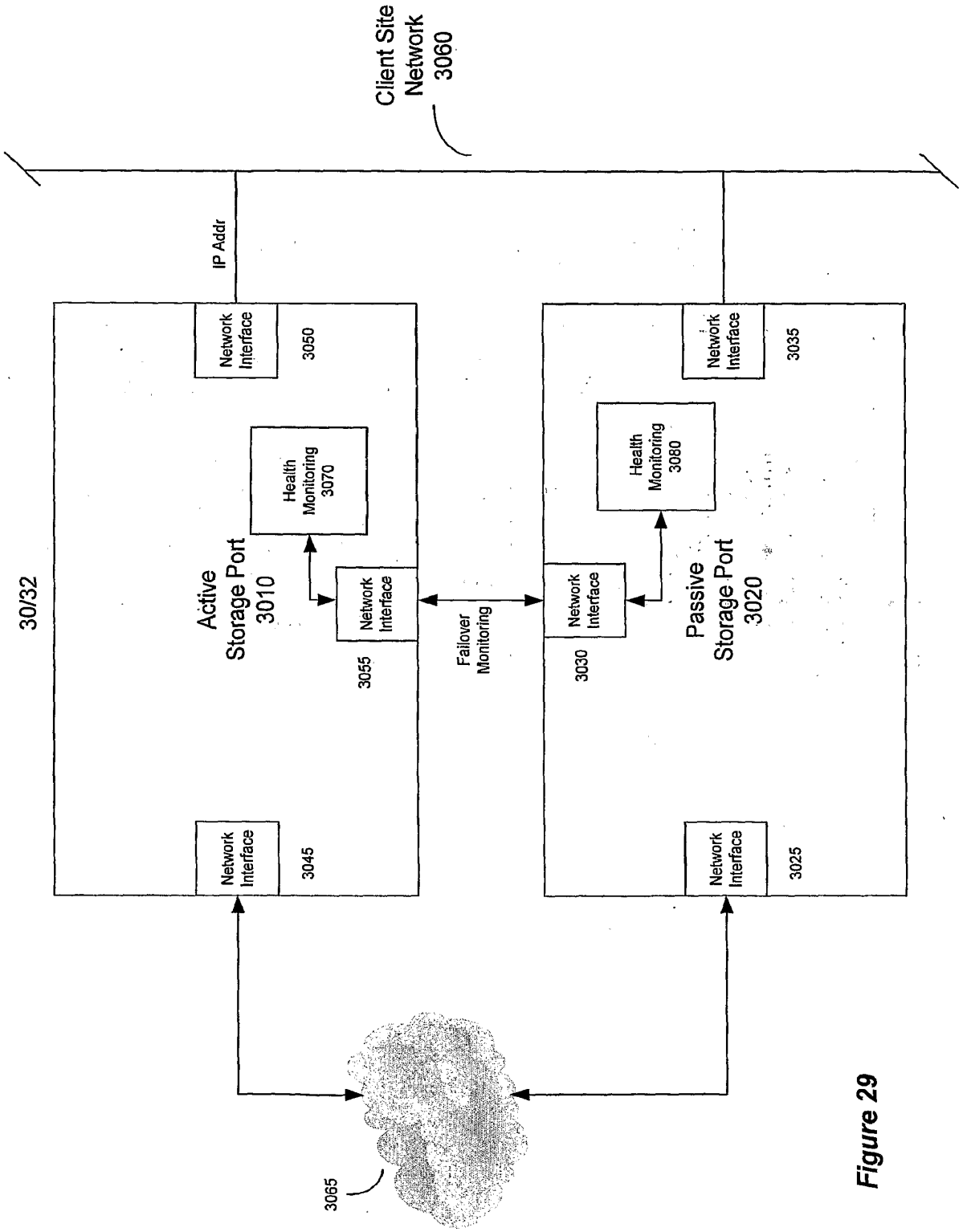

Client Site Network 3060
IP Addr
Network Interface
3050
Health Monitoring 3070
Active Storage Port 3010
Network Interface
3055
Failover Monitoring
Network Interface
3030
Health Monitoring 3080
Passive Storage Port 3020
Network Interface
3035
Network Interface
3045
Network Interface
3025
30/32
3065

Figure 29

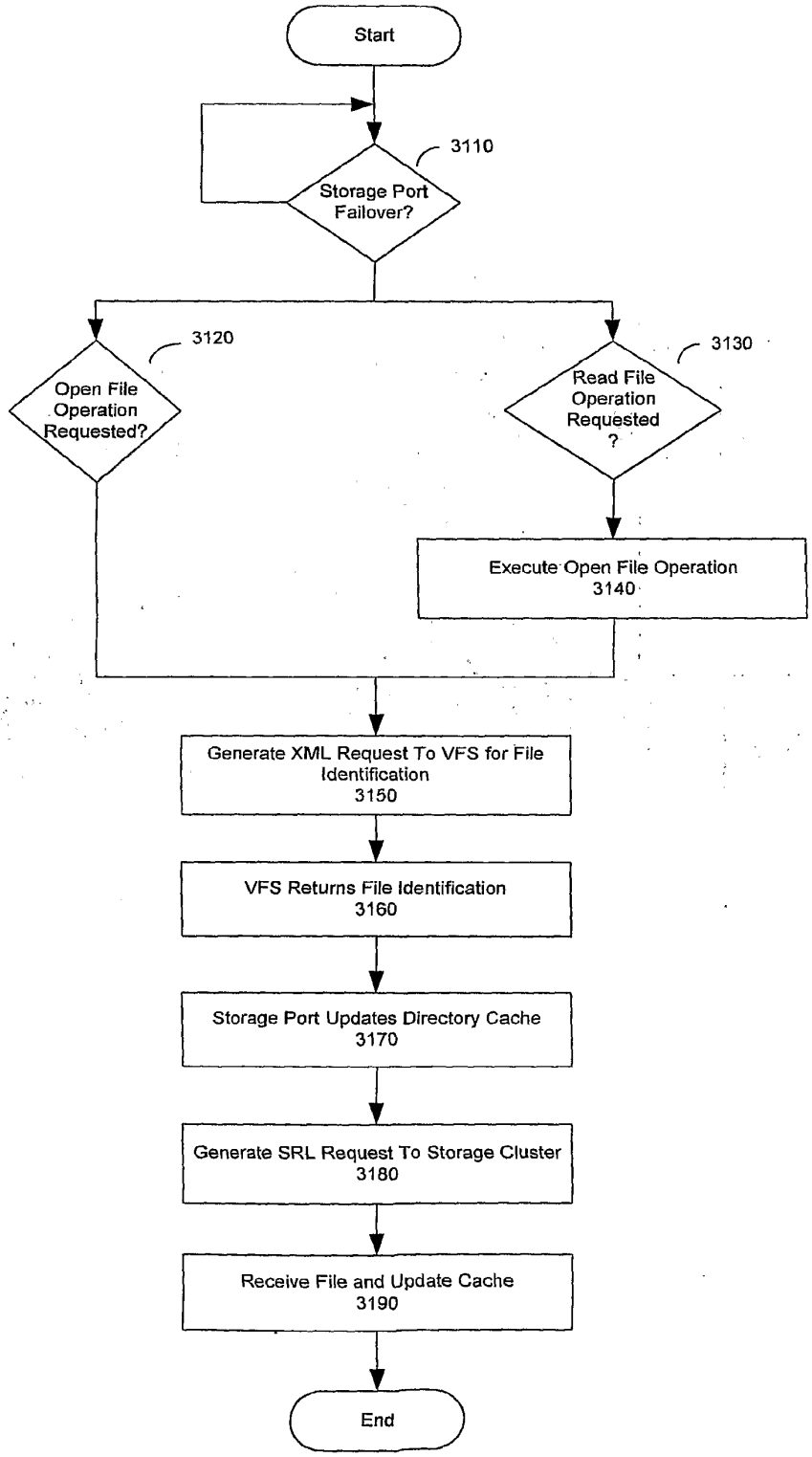

Start
3110
Storage Port Failover?
3120
Open File Operation Requested?
3130
Read File Operation Requested ?
Execute Open File Operation 3140
Generate XML Request To VFS for File Identification 3150
VFS Returns File Identification 3160
Storage Port Updates Directory Cache 3170
Generate SRL Request To Storage Cluster 3180
Receive File and Update Cache 3190
End

Figure 30

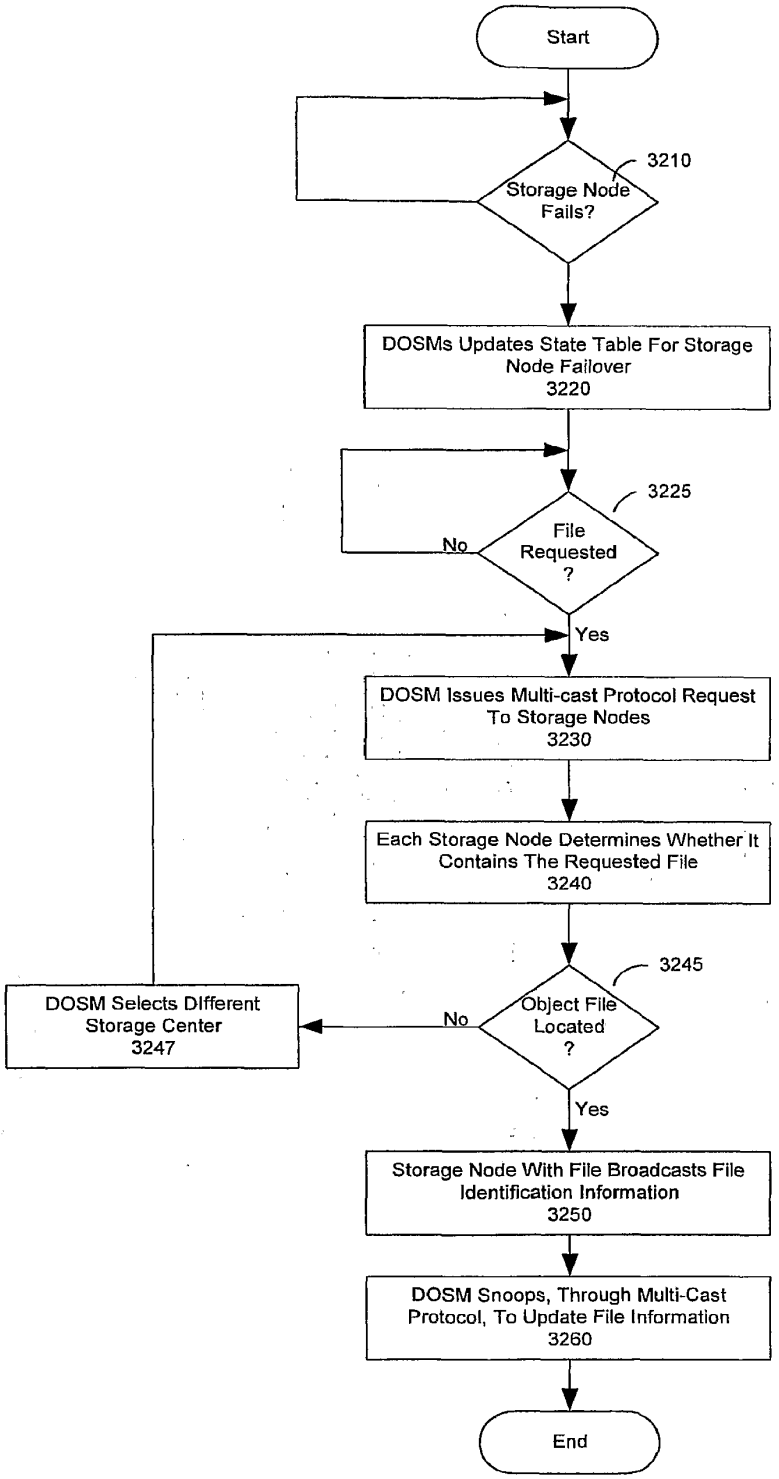

Start
3210
Storage Node Fails?
DOSMs Updates State Table For Storage Node Failover
3220
3225
File Requested ?
No
Yes
DOSM Issues Multi-cast Protocol Request To Storage Nodes
3230
Each Storage Node Determines Whether It Contains The Requested File
3240
3245
Object File Located ?
No
DOSM Selects Different Storage Center
3247
Yes
Storage Node With File Broadcasts File Identification Information
3250
DOSM Snoops, Through Multi-Cast Protocol, To Update File Information
3260
End

Figure 31

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 204 277 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.05.2002 Bulletin 2002/19

(51) Int Cl.[7]: **H04N 7/24**

(21) Application number: **01308791.1**

(22) Date of filing: **16.10.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **06.11.2000 US 707520**

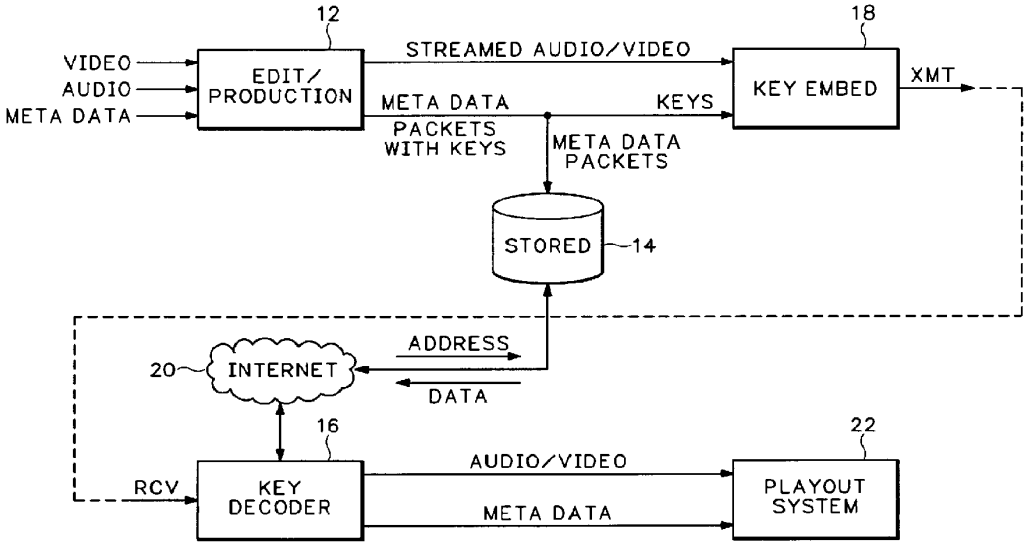
(71) Applicant: **Tektronix, Inc.**
Beaverton, OR 97077 (US)

(72) Inventor: **Limaye, Ajit M.**
Hillsboro, Oregon 97124 (US)

(74) Representative: **Molyneaux, Martyn William**
Wildman, Harrold, Allen & Dixon
11th Floor, Tower 3,
Clements Inn,
London WC2A 2AZ (GB)

(54) Subliminally embedded keys in video for synchronization

(57) A data file containing metadata and/or control data is synchronized with associated audio/video data by subliminally embedding a key in a frame of the audio/video. The key indicates the location of the data file and a time after the embedded frame in which the data file is to be activated to be in synchronism with the audio/video. The data file is accessed via an alternate channel and held in a buffer until the time indicated by the key. The metadata from the data file is played out for display in synchronism with the associated audio/video data, and instructions contained in the control data are executed in synchronism with the associated audio/video data.



EP 1 204 277 A2

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND OF THE INVENTION

[0001] The present invention relates to multimedia systems, and more particularly to a subliminally embedded key in a video signal for synchronization of playout control of multimedia data and/or of execution of instructions contained in control data.

[0002] Watermarking of video signals is becoming of increasing use as a means of transmitting very low rate data as part of the video signal. Watermarking of video has been proposed for performing audio to video delay compensation, for indicating authentication or program ownership and for verifying playing of a video signal such as in advertisement logging. The watermarking technique inserts the very low rate data into the active portion of the video signal so as to be invisible while still having the robustness to survive video signal processing including multiple generations of compression encoding/decoding. See U.S. Patent No. 4,969,041 issued to William O'Grady et al on November 6, 1990 entitled "Embedment of Data in a Video Signal" and co-pending U.S. Patent Application Serial No. 08/829,524 by Daniel Baker et al filed on March 28, 1997 entitled "Transparent Embedment of Data in a Video Signal".

[0003] Also the use of auxiliary channels for transmitting data related to video signals is known, as shown in U.S. Patent No. 6,075,561 issued to Bozidar Janko on June 13, 2000 entitled "Low Duty-Cycle Transport of Video Reference Images". With the advent of the Internet, proposals have been made to use the Internet as the auxiliary channel for transporting data. It is anticipated that when video that is streamed over the Internet is played out, it may be desirable to also play out other data — called metadata — that is associated with the video to immerse the viewer in the experience. It may also be desirable to transmit control data to the equipment receiving the video. This control data may be used for one or more of the following purposes: (1) cue a commercial; (2) specify a destination to which the video is to be routed; (3) control auxiliary equipment to actuate other sensory cues such as activation of special lighting or sound effects; (4) control the parameters for compressing the video prior to storage; etc.

[0004] However transmitting the metadata is not currently possible using watermarking technology with video. The bit rate of the metadata, such as 9600 baud, is too high for the very low data rate channel afforded by watermarking. Transmission of control data may or may not be possible using watermarking technology directly, depending upon the quantity of data which varies with the application.

[0005] The problem that arises is how to synchronize the metadata or other control data with the video when they are transmitted over different channels so that the metadata appears at the proper point with relationship to the video when seen by the viewer, or the control data is retrieved and used at the proper point with relationship to the video.

[0006] What is desired is a means for synchronizing the metadata or control data with the associated video when the video is played out.

BRIEF SUMMARY OF THE INVENTION

[0007] Accordingly the present invention provides subliminally embedded keys in video that act as pointers and synchronizing signals for a data file containing metadata and/or control data so that the metadata is displayed with the video and/or instructions contained in the control data are executed at the proper time. At the transmission end of a system a key is generated in synchronization with the video, the key being associated with corresponding data file. The key is embedded subliminally in the video at an appropriate point using watermarking techniques. At a receiver the key is decoded from the video and used to access a network server that contains the data file. Once retrieved the metadata from the data file is displayed with the video at a point in synchronization with the video as indicated by the key, or the control data is used to perform one or more auxiliary functions at designated times. For small data files where the retrieval delay is small, the key may be just a few frames before the first video frame which is associated with the data file, while for large data files the key may be inserted several seconds before the first video frame which is associated with the data file. The key provides both an "address" for retrieving the data file and a time from the key frame when the metadata from the data file is to be played out with the video for a viewer or when the instructions contained in the control data are to be executed. In this way the data file is synchronized with the video.

[0008] The objects, advantages and other novel features of the present invention are apparent from the following detailed description when read in conjunction with the appended claims and attached drawing.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

[0009] The Figure is a block diagram view of a system for synchronizing a data file with video using subliminally embedded keys according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0010] Referring now to the Figure video, audio and an associated data file containing metadata and/or control data is input to an edit/production system **12.** The output from the edit/production system **12** is streamed audio/video and the data file with associated keys. The data file is stored in an appropriate storage device **14**, such as a network server, and the keys are input with the streaming audio/video to a key embedment system

Ex.1002 / Page 462 of 1385
APPLE INC.

16 such as those described in U.S. Patent No. 4,969,041 and U.S. Patent Application Serial No. 08/829,524 referenced above. The keys have information that indicates the location of the associated data file in the storage medium **14** and a time in number of frames from the frame in which the key is embedded when the control instructions from the data file should be executed or the metadata should be played out to be in synchronism with the audio/video stream to account for latency in accessing the data file. Large data files require a longer access time, so the key is embedded in a frame much further ahead of the frame where the data file is to be used, whereas small data files may not require as much "lead" time.

[0011] The streaming audio/video with embedded keys is transmitted over a transmit channel to a receive site where a key decoder **18** extracts the keys from the streaming audio/video and accesses an alternate channel **20**, such as the Internet. The information from the keys is transmitted over the alternate channel **20** to the storage medium **14** and the data file is transferred from the storage medium to a buffer in the key decoder **18**. When the number of frames from the frame in which the key is embedded has passed, as indicated by the key, the metadata from the data file is played out with the streaming audio/video to a playout system **22** so as to be synchronized with the audio/video stream. Alternatively the instructions contained in the control data of the data file are executed. The playout system **22** may be a set top box for a consumer television set or multimedia computer where the viewer can control whether or not to view the metadata or only portions of the metadata. The playout system **22** may also be the device responsible for implementing the instructions contained in the control data.

[0012] Thus the present invention provides subliminally embedded keys in video for synchronization of a data file containing metadata and/or control data with associated audio/video streams, the data file being provided by an alternate channel and the keys having an address for the data file as well as a time when the metadata in the data file plays out with the audio/video streams or when the instructions in the control data are executed.

Claims

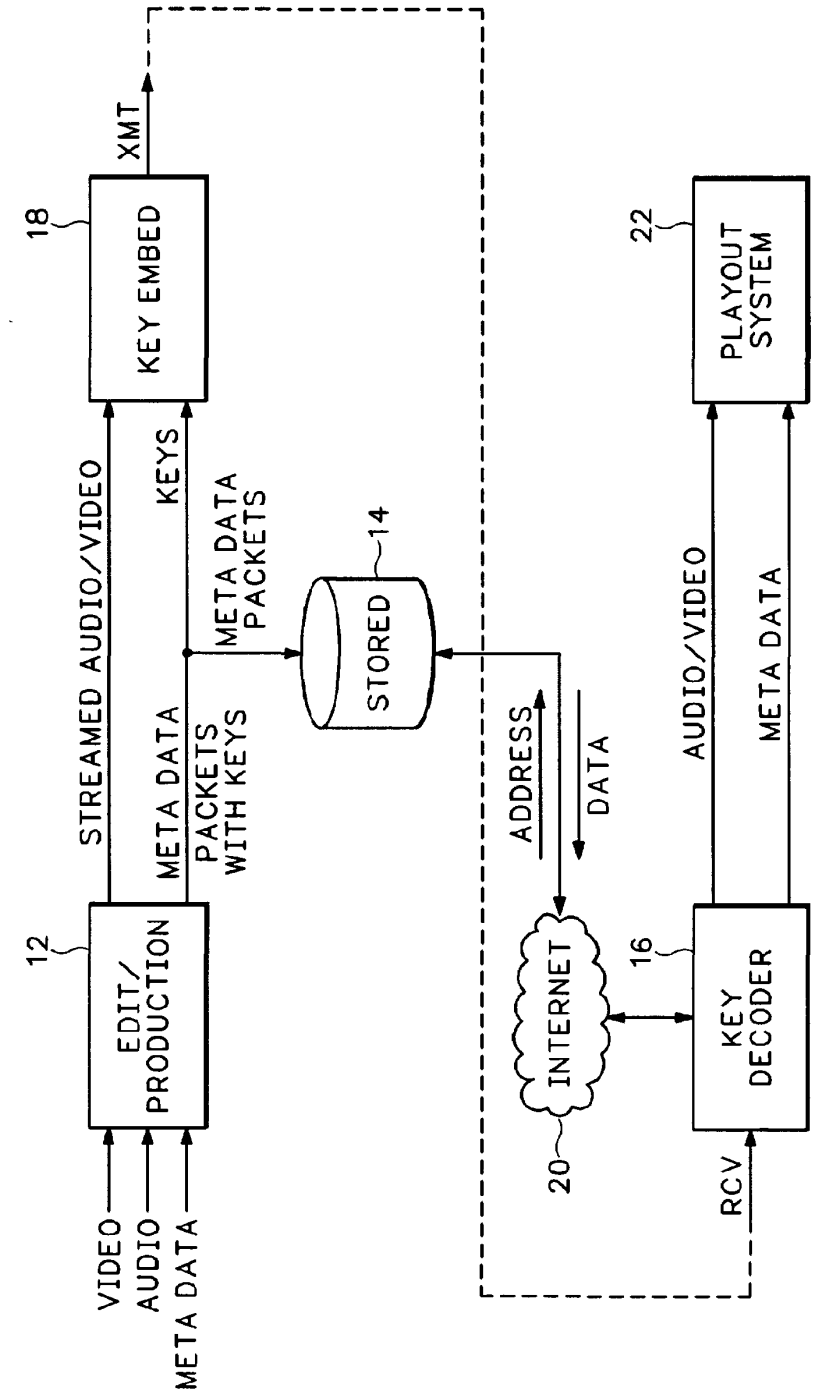
1. A method of synchronizing a data file with associated audio/video data using subliminally embedded keys comprising the steps of:

   at a transmit site embedding a key subliminally in the audio/video data, the key indicating a location of the data file on a network storage medium and a latency time;
   at a receive site extracting the key from the audio/video data;
   accessing the network storage medium according to the location indicated by the key;
   using the data file in synchronism with the audio/video data according to the latency time.

2. The method as recited in claim 1 wherein the data file comprises metadata to be played out in synchronism with the associated audio/video data and the using step comprises the step of playing out the metadata for display in synchronism with the audio/video data.

3. The method as recited in claim 1 wherein the data file comprises control data to be activated in synchronism with the associated audio/video data and the using step comprises the step of activating instructions contained in the control data for execution in synchronism with the audio/video data.

Ex.1002 / Page 463 of 1385
APPLE INC.


VIDEO
AUDIO
META DATA
12
EDIT/ PRODUCTION
STREAMED AUDIO/VIDEO
META DATA PACKETS WITH KEYS
KEYS
META DATA PACKETS
18
KEY EMBED
XMT
14
STORED
ADDRESS
DATA
20
INTERNET
16
KEY DECODER
RCV
AUDIO/VIDEO
META DATA
22
PLAYOUT SYSTEM

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 9/36 — A1

(11) International Publication Number: **WO 97/43736**

(43) International Publication Date: 20 November 1997 (20.11.97)

(21) International Application Number: PCT/US97/08351

(22) International Filing Date: 16 May 1997 (16.05.97)

(30) Priority Data:

08/649,419	16 May 1996 (16.05.96)	US
08/746,613	12 November 1996 (12.11.96)	US

(60) Parent Applications or Grants
(63) Related by Continuation
US 08/649,419 (CIP)
Filed on 16 May 1996 (16.05.96)
US 08/746,613 (CIP)
Filed on 12 November 1996 (12.11.96)

(71) Applicant *(for all designated States except US)*: DIGIMARC CORPORATION [US/US]; 521 S.W. 11th Avenue #200, Portland, OR 97205 (US).

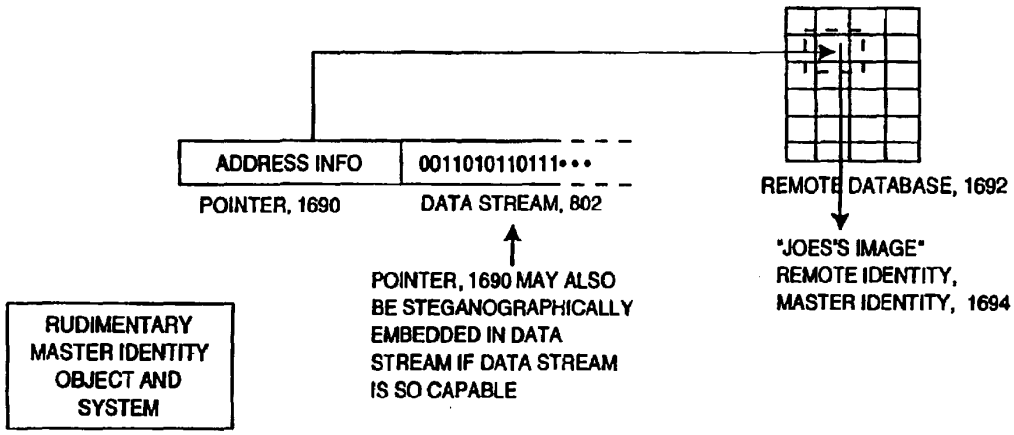
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: RHOADS, Geoffrey, B. [US/US]; 304 S.W. Tualatin Loop, West Linn, OR 97068 (US).

(74) Agents: JOHNSON, Alexander, C., Jr. et al.; Marger, Johnson, McCollom & Stolowitz, 1030 S.W. Morrison Street, Portland, OR 97205 (US).

(81) Designated States: AU, CA, JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: COMPUTER SYSTEM LINKED BY USING INFORMATION IN DATA OBJECTS



(57) Abstract

Various improvements to steganographic systems, and applications therefore, are disclosed. The improvements include facilitating scale and rotation registration for steganographic decoding by use of rotationally symmetric steganographically embedded patterns and subliminal digital graticules; improved techniques for decoding without access to unencoded originals; improving robustness of steganographic coding in motion pictures and/or in the presence of lossy compression/decompression; and representing data (1690) by patterned bit cells (802) whose energy in the spatial domain facilitates decoding registration (1692). Applications include enhanced-security financial transactions, counterfeit resistant identification cards, fraud deterrent systems for cellular telephony, covert modem channels in video transmissions, photo duplication kiosks with automatic copyright detection, and hotlinked image objects (e.g., with embedded URLs) for use on the Internet.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

COMPUTER SYSTEM LINKED BY USING INFORMATION IN DATA OBJECTS

Background of the Invention

Hiding data in imagery or audio is a technique well known to artisans in the field, and is termed "steganography." There are a number of diverse approaches to, and applications of, steganography. A brief survey follows:

British patent publication 2,196,167 to Thorn EMI discloses a system in which an audio recording is electronically mixed with a marking signal indicative of the owner of the recording, where the combination is perceptually identical to the original. U.S. patents 4,963,998 and 5,079,648 disclose variants of this system.

U.S. Patent 5,319,735 to Bolt, Berenak & Newman rests on the same principles as the earlier Thorn EMI publication, but additionally addresses psycho-acoustic masking issues.

U.S. Patents 4,425,642, 4,425,661, 5,404,377 and 5,473,631 to Moses disclose various systems for imperceptibly embedding data into audio signals -- the latter two patents particularly focusing on neural network implementations and perceptual coding details.

U.S. Patent 4,943,973 to AT&T discloses a system employing spread spectrum techniques for adding a low level noise signal to other data to convey auxiliary data therewith. The patent is particularly illustrated in the context of transmitting network control signals along with digitized voice signals.

U.S. Patent 5,161,210 to U.S. Philips discloses a system in which additional low-level quantization levels are defined on an audio signal to convey, e.g., a copy inhibit code, therewith.

U.S. Patent 4,972,471 to Gross discloses a system intended to assist in the automated monitoring of audio (e.g. radio) signals for copyrighted materials by reference to identification signals subliminally embedded therein.

U.S. Patent 5,243,423 to DeJean discloses a video steganography system which encodes digital data (e.g. program syndication verification, copyright marking, media research, closed captioning, or like data) onto randomly selected video lines. DeJean relies

on television sync pulses to trigger a stored pseudo random sequence which is XORed with the digital data and combined with the video.

European application EP 581,317 discloses a system for redundantly marking images with multi-bit identification codes. Each "1" ("0") bit of the code is manifested as a slight increase (decrease) in pixel values around a plurality of spaced apart "signature points." Decoding proceeds by computing a difference between a suspect image and the original, unencoded image, and checking for pixel perturbations around the signature points.

PCT application WO 95/14289 describes the present applicant's prior work in this field.

Komatsu et al., describe an image marking technique in their paper "A Proposal on Digital Watermark in Document Image Communication and Its Application to Realizing a Signature," Electronics and Communications in Japan, Part 1, Vol. 73, No. 5, 1990, pp. 22-33. The work is somewhat difficult to follow but apparently results in a simple yes/no determination of whether the watermark is present in a suspect image (e.g. a 1 bit encoded message).

Others embed the information "in-band" (i.e. in the visible video signal itself). Examples include U.S. Patents 4,528,588, 4,595,950, and 5,319,453; European application 441,702; and Matsui et. al, "Video-Steganography: How to Secretly Embed a Signature in a Picture," IMA Intellectual Property Project Proceedings, January 1994, Vol. 1, Issue 1, pp. 187-205.

Copyright marking of video and multimedia is found in "Access Control and Copyright Protection for Images (ACCOPI), WorkPackage 8: Watermarking," June 30, 1995, 46 pages. TALISMAN, appears to extend certain of the ACCOPI work.

A British company, Highwater FBI, Ltd., has introduced a software product which is said to imperceptibly embed identifying information into photographs and other graphical images. This technology is the subject of European patent applications 9400971.9 (filed January 19, 1994), 9504221.2 (filed March 2, 1995), and 9513790.7 (filed July 3, 1995), the first of which has been laid open as PCT publication WO 95/20291.

Brief Description Of The Drawings

Fig. 1 is a simple and classic depiction of a one dimensional digital signal which is discretized in both axes.

Fig. 2 is a general overview, with detailed description of steps, of the process of embedding an "imperceptible" identification signal onto another signal.

Fig. 3 is a step-wise description of how a suspected copy of an original is identified.

Fig. 4 is a schematic view of an apparatus for pre-exposing film with identification information.

Fig. 5 is a diagram of a "black box" embodiment.

Fig. 6 is a schematic block diagram of the embodiment of Fig. 5.

Fig. 7 shows a variant of the Fig. 6 embodiment adapted to encode successive sets of input data with different code words but with the same noise data.

Fig. 8 shows a variant of the Fig. 6 embodiment adapted to encode each frame of a videotaped production with a unique code number.

Figs. 9A-9C are representations of an industry standard noise second.

Fig. 10 shows an integrated circuit used in detecting standard noise codes.

Fig. 11 shows a process flow for detecting a standard noise code that can be used in the Fig. 10 embodiment.

Fig. 12 is an embodiment employing a plurality of detectors.

Fig. 13 shows an embodiment in which a pseudo-random noise frame is generated from an image.

Fig. 14 illustrates how statistics of a signal can be used in aid of decoding.

Fig. 15 shows how a signature signal can be preprocessed to increase its robustness in view of anticipated distortion, e.g. MPEG.

Figs. 16 and 17 show embodiments in which information about a file is detailed both in a header, and in the file itself.

Figs. 18-20 show details of embodiments using rotationally symmetric patterns.

Fig. 21 shows encoding "bumps" rather than pixels.

Figs. 22-26 detail aspects of a security card.

Fig. 27 is a diagram illustrating a network linking method using information embedded in data objects that have inherent noise.

Figs. 27A and 27B show a typical web page, and a step in its encapsulation into a self extracting web page object.

Fig. 28 is a diagram of a photographic identification document or security card.

Figs. 29 and 30 illustrate two embodiments by which subliminal digital graticules can be realized.

Fig. 29A shows a variation on the Fig. 29 embodiment.

Figs. 31A and 31B show the phase of spatial frequencies along two inclined axes.

Figs. 32A - 32C show the phase of spatial frequencies along first, second and third concentric rings.

Figs 33A - 33E show steps in the registration process for a subliminal graticule using inclined axes.

Figs. 34A - 34E show steps in the registration process for a subliminal graticule using concentric rings.

Figs. 35A - 35C shows further steps in the registration process for a subliminal graticule using inclined axes.

Figs. 36A - 36D show another registration process that does not require a 2D FFT.

Fig. 37 is a flow chart summarizing a registration process for subliminal graticules.

Fig. 38 is a block diagram showing principal components of an exemplary wireless telephony system.

Fig. 39 is a block diagram of an exemplary steganographic encoder that can be used in the telephone of the Fig. 38 system.

Fig. 40 is a block diagram of an exemplary steganographic decoder that can be used in the cell site of the Fig. 1 system.

Figs. 41A and 41B show exemplary bit cells used in one form of encoding.

Fig. 42 shows a hierarchical arrangement of signature blocks, sub-blocks, and bit cells used in one embodiment.

Fig. 43 shows a general overview of a computer system linked by using information embedded in the objects.

Figs. 44-59 are representative computer screens generated in accordance with the present invention.

Fig. 60 is a basic overview of how a traditional file header can be replaced by a pointer to a database location where header information resides.

Fig. 61 expands on Fig. 60 by illustrating that a pointer to a remote location can coexist with existing data file formats which might include headers.

Fig. 62 is a basic map showing how an instrument or application can associate a pointer attached to an object to some remote digital storage location.

Fig. 63 is a condensed depiction of a process that an instrument or application might go through in resolving and acting upon remote information pointed to by an attached pointer.

Fig. 64 graphically illustrates that attached information can actually be sequences of actions or multiple sets of information.

Fig. 65 shows how the basic principles of master identity objects can be used to fuel a reporting network wherein a central location can "keep track" of where its copies migrate.

Detailed Description

In the following discussion of an illustrative embodiment, the words "signal" and "image" are used interchangeably to refer to both one, two, and even beyond two dimensions of digital signal. Examples will routinely switch back and forth between a one dimensional audio-type digital signal and a two dimensional image-type digital signal.

In order to fully describe the details of an illustrative embodiment, it is necessary first to describe the basic properties of a digital signal. Fig. 1 shows a classic representation of a one dimensional digital signal. The x-axis defines the index numbers of sequence of digital "samples," and the y-axis is the instantaneous value of the signal at that sample, being constrained to exist only at a finite number of levels defined as the "binary depth" of a digital sample. The example depicted in Fig. 1 has the value of 2 to the fourth power, or "4 bits," giving 16 allowed states of the sample value.

For audio information such as sound waves, it is commonly accepted that the digitization process discretizes a continuous phenomena both in the time domain and in the signal level domain. As such, the process of digitization itself introduces a fundamental error source, in that it cannot record detail smaller than the discretization interval in either domain. The industry has referred to this, among other ways, as "aliasing" in the time domain, and "quantization noise" in the signal level domain. Thus, there will always be a basic error floor of a digital signal. Pure quantization noise, measured in a root mean square sense, is theoretically known to have the value of one over the square root of twelve, or about 0.29 DN, where DN stands for 'Digital Number' or the finest unit increment of the signal level. For example, a perfect 12-bit digitizer will have 4096 allowed DN with an innate root mean square noise floor of ~0.29 DN.

All known physical measurement processes add additional noise to the transformation of a continuous signal into the digital form. The quantization noise typically adds in quadrature (square root of the mean squares) to the "analog noise" of the measurement process, as it is sometimes referred to.

With almost all commercial and technical processes, the use of the decibel scale is used as a measure of signal and noise in a given recording medium. The expression "signal-to-noise ratio" is generally used, as it will be in this disclosure. As an example, this disclosure refers to signal to noise ratios in terms of signal power and noise power, thus 20 dB represents a 10 times increase in signal amplitude.

In summary, this embodiment embeds an N-bit value onto an entire signal through the addition of a very low amplitude encodation signal which has the look of pure noise. N is usually at least 8 and is capped on the higher end by ultimate signal-to-noise considerations and "bit error" in retrieving and decoding the N-bit value. As a practical matter, N is chosen based on application specific considerations, such as the number of unique different "signatures" that are desired. To illustrate, if N=128, then the number of unique digital signatures is in excess of 10^^38 (2^^128). This number is believed to be more than adequate to both identify the material with sufficient statistical certainty and to index exact sale and distribution information.

The amplitude or power of this added signal is determined by the aesthetic and informational considerations of each and every application using the present methodology. For instance, non-professional video can stand to have a higher embedded signal level without becoming noticeable to the average human eye, while high precision audio may only be able to accept a relatively small signal level lest the human ear perceive an objectionable increase in "hiss." These statements are generalities and each application has its own set of criteria in choosing the signal level of the embedded identification signal. The higher the level of embedded signal, the more corrupted a copy can be and still be identified. On the other hand, the higher the level of embedded signal, the more objectionable the perceived noise might be, potentially impacting the value of the distributed material.

To illustrate the range of different applications to which applicant's technology can be applied, the present specification details two different systems. The first (termed, for lack of a better name, a "batch encoding" system), applies identification coding to an existing data signal. The second (termed, for lack of a better name, a "real time encoding" system), applies identification coding to a signal as it is produced. Those skilled in the art will recognize that the principles of applicant's technology can be applied in a number of other contexts in addition to these particularly described.

The discussions of these two systems can be read in either order. Some readers may find the latter more intuitive than the former; for others the contrary may be true.

BATCH ENCODING

The following discussion of a first class of embodiments is best prefaced by a section defining relevant terms:

The original signal refers to either the original digital signal or the high quality digitized copy of a non-digital original.

The N-bit identification word refers to a unique identification binary value, typically having N range anywhere from 8 to 128, which is the identification code ultimately placed onto the original signal via the disclosed transformation process. In the illustrated embodiment, each N-bit identification word begins with the sequence of values '0101,' which is used to determine an optimization of the signal-to-noise ratio in the identification procedure of a suspect signal (see definition below).

The m'th bit value of the N-bit identification word is either a zero or one corresponding to the value of the m'th place, reading left to right, of the N-bit word. E.g., the first (m=1) bit value of the N=8 identification word 01110100 is the value '0;' the second bit value of this identification word is '1', etc.

The m'th individual embedded code signal refers to a signal which has dimensions and extent precisely equal to the original signal (e.g. both are a 512 by 512 digital image), and which is (in the illustrated embodiment) an independent pseudo-random sequence of digital values. "Pseudo" pays homage to the difficulty in philosophically defining pure randomness, and also indicates that there are various acceptable ways of generating the "random" signal. There will be exactly N individual embedded code signals associated with any given original signal.

The acceptable perceived noise level refers to an application-specific determination of how much "extra noise," i.e. amplitude of the composite embedded code signal described next, can be added to the original signal and still have an acceptable signal to sell or otherwise distribute. This disclosure uses a 1 dB increase in noise as a typical value which might be acceptable, but this is quite arbitrary.

The composite embedded code signal refers to the signal which has dimensions and extent precisely equal to the original signal, (e.g. both are a 512 by 512 digital image), and which contains the

addition and appropriate attenuation of the N individual embedded code signals. The individual embedded signals are generated on an arbitrary scale, whereas the amplitude of the composite signal must not exceed the pre-set acceptable perceived noise level, hence the need for "attenuation" of the N added individual code signals.

The distributable signal refers to the nearly similar copy of the original signal, consisting of the original signal plus the composite embedded code signal. This is the signal which is distributed to the outside community, having only slightly higher but acceptable "noise properties" than the original.

A suspect signal refers to a signal which has the general appearance of the original and distributed signal and whose potential identification match to the original is being questioned. The suspect signal is then analyzed to see if it matches the N-bit identification word.

The detailed methodology of this first embodiment begins by stating that the N-bit identification word is encoded onto the original signal by having each of the m bit values multiply their corresponding individual embedded code signals, the resultant being accumulated in the composite signal, the fully summed composite signal then being attenuated down to the acceptable perceived noise amplitude, and the resultant composite signal added to the original to become the distributable signal.

The original signal, the N-bit identification word, and all N individual embedded code signals are then stored away in a secured place. A suspect signal is then found. This signal may have undergone multiple copies, compressions and decompressions, resamplings onto different spaced digital signals, transfers from digital to analog back to digital media, or any combination of these items. IF the signal still appears similar to the original, i.e. its innate quality is not thoroughly destroyed by all of these transformations and noise additions, then depending on the signal to noise properties of the embedded signal, the identification process should function to some objective degree of statistical confidence. The extent of corruption of the suspect signal and the original acceptable perceived noise level are two key parameters in determining an expected confidence level of identification.

The identification process on the suspected signal begins by resampling and aligning the suspected signal onto the digital format and extent of the original signal. Thus, if an image has been reduced by a factor of two, it needs to be digitally enlarged by that same factor. Likewise, if a piece of music has been "cut out," but may still have the same sampling rate as the original, it is necessary to register this cut-out piece to the original, typically done by performing a local digital cross-correlation of the two signals (a common digital operation), finding at what delay value the correlation peaks, then using this found delay value to register the cut piece to a segment of the original.

Once the suspect signal has been sample-spacing matched and registered to the original, the signal levels of the suspect signal should be matched in an rms sense to the signal level of the original. This can be done via a search on the parameters of offset, amplification, and gamma being optimized by using the

minimum of the mean squared error between the two signals as a function of the three parameters. We can call the suspect signal normalized and registered at this point, or just normalized for convenience.

The newly matched pair then has the original signal subtracted from the normalized suspect signal to produce a difference signal. The difference signal is then cross-correlated with each of the N individual embedded code signals and the peak cross-correlation value recorded. The first four bit code ('0101') is used as a calibrator both on the mean values of the zero value and the one value, and on further registration of the two signals if a finer signal to noise ratio is desired (i.e., the optimal separation of the 0101 signal will indicate an optimal registration of the two signals and will also indicate the probable existence of the N-bit identification signal being present.)

The resulting peak cross-correlation values will form a noisy series of floating point numbers which can be transformed into 0's and 1's by their proximity to the mean values of 0 and 1 found by the 0101 calibration sequence. If the suspect signal has indeed been derived from the original, the identification number resulting from the above process will match the N-bit identification word of the original, bearing in mind either predicted or unknown "bit error" statistics. Signal-to-noise considerations will determine if there will be some kind of "bit error" in the identification process, leading to a form of X% probability of identification where X might be desired to be 99.9% or whatever. If the suspect copy is indeed not a copy of the original, an essentially random sequence of 0's and 1's will be produced, as well as an apparent lack of separation of the resultant values. This is to say, if the resultant values are plotted on a histogram, the existence of the N-bit identification signal will exhibit strong bi-level characteristics, whereas the non-existence of the code, or the existence of a different code of a different original, will exhibit a type of random gaussian-like distribution. This histogram separation alone should be sufficient for an identification, but it is even stronger proof of identification when an exact binary sequence can be objectively reproduced.

Specific Example

Imagine that we have taken a valuable picture of two heads of state at a cocktail party, pictures which are sure to earn some reasonable fee in the commercial market. We desire to sell this picture and ensure that it is not used in an unauthorized or uncompensated manner. This and the following steps are summarized in Fig. 2.

Assume the picture is transformed into a positive color print. We first scan this into a digitized form via a normal high quality black and white scanner with a typical photometric spectral response curve. (It is possible to get better ultimate signal to noise ratios by scanning in each of the three primary colors of the color image, but this nuance is not central to describing the basic process.)

Let us assume that the scanned image now becomes a 4000 by 4000 pixel monochrome digital image with a grey scale accuracy defined by 12-bit grey values or 4096 allowed levels. We will call this the "original digital image" realizing that this is the same as our "original signal" in the above definitions.

During the scanning process we have arbitrarily set absolute black to correspond to digital value '30'. We estimate that there is a basic 2 Digital Number root mean square noise existing on the original digital image, plus a theoretical noise (known in the industry as "shot noise") of the square root of the brightness value of any given pixel. In formula, we have:

$$<\text{RMS Noise}_{n,m}> = \text{sqrt}(4 + (V_{n,m}-30)) \quad (1)$$

Here, n and m are simple indexing values on rows and columns of the image ranging from 0 to 3999. Sqrt is the square root. V is the DN of a given indexed pixel on the original digital image. The < > brackets around the RMS noise merely indicates that this is an expected average value, where it is clear that each and every pixel will have a random error individually. Thus, for a pixel value having 1200 as a digital number or "brightness value", we find that its expected rms noise value is sqrt(1204) = 34.70, which is quite close to 34.64, the square root of 1200.

We furthermore realize that the square root of the innate brightness value of a pixel is not precisely what the eye perceives as a minimum objectionable noise, thus we come up with the formula:

$$<\text{RMS Addable Noise}_{n,m}> = X*\text{sqrt}(4+(V_{n,m}-30)\text{^}Y) \quad (2)$$

Where X and Y have been added as empirical parameters which we will adjust, and "addable" noise refers to our acceptable perceived noise level from the definitions above. We now intend to experiment with what exact value of X and Y we can choose, but we will do so at the same time that we are performing the next steps in the process.

The next step in our process is to choose N of our N-bit identification word.' We decide that a 16 bit main identification value with its 65536 possible values will be sufficiently large to identify the image as ours, and that we will be directly selling no more than 128 copies of the image which we wish to track, giving 7 bits plus an eighth bit for an odd/even adding of the first 7 bits (i.e. an error checking bit on the first seven). The total bits required now are at 4 bits for the 0101 calibration sequence, 16 for the main identification, 8 for the version, and we now throw in another 4 as a further error checking value on the first 28 bits, giving 32 bits as N. The final 4 bits can use one of many industry standard error checking methods to choose its four values.

We now randomly determine the 16 bit main identification number, finding for example, 1101 0001 1001 1110; our first versions of the original sold will have all 0's as the version identifier, and the

error checking bits will fall out where they may. We now have our unique 32 bit identification word which we will embed on the original digital image.

To do this, we generate 32 independent random 4000 by 4000 encoding images for each bit of our 32 bit identification word. The manner of generating these random images is revealing. There are numerous ways to generate these. By far the simplest is to turn up the gain on the same scanner that was used to scan in the original photograph, only this time placing a pure black image as the input, then scanning this 32 times. The only drawback to this technique is that it does require a large amount of memory and that "fixed pattern" noise will be part of each independent "noise image." But, the fixed pattern noise can be removed via normal "dark frame" subtraction techniques. Assume that we set the absolute black average value at digital number '100,' and that rather than finding a 2 DN rms noise as we did in the normal gain setting, we now find an rms noise of 10 DN about each and every pixel's mean value.

We next apply a mid-spatial-frequency bandpass filter (spatial convolution) to each and every independent random image, essentially removing the very high and the very low spatial frequencies from them. We remove the very low frequencies because simple real-world error sources like geometrical warping, splotches on scanners, mis-registrations, and the like will exhibit themselves most at lower frequencies also, and so we want to concentrate our identification signal at higher spatial frequencies in order to avoid these types of corruptions. Likewise, we remove the higher frequencies because multiple generation copies of a given image, as well as compression-decompression transformations, tend to wipe out higher frequencies anyway, so there is no point in placing too much identification signal into these frequencies if they will be the ones most prone to being attenuated. Therefore, our new filtered independent noise images will be dominated by mid-spatial frequencies. On a practical note, since we are using 12-bit values on our scanner and we have removed the DC value effectively and our new rms noise will be slightly less than 10 digital numbers, it is useful to boil this down to a 6-bit value ranging from -32 through 0 to 31 as the resultant random image.

Next we add all of the random images together which have a '1' in their corresponding bit value of the 32-bit identification word, accumulating the result in a 16-bit signed integer image. This is the unattenuated and un-scaled version of the composite embedded signal.

Next we experiment visually with adding the composite embedded signal to the original digital image, through varying the X and Y parameters of equation 2. In formula, we visually iterate to both maximize X and to find the appropriate Y in the following:

$$V_{dist;n,m} = V_{orig;n,m} + V_{comp;n,m} * X * \mathrm{sqrt}(4 + V_{orig;n,m} \hat{} Y) \qquad (3)$$

where dist refers to the candidate distributable image, i.e. we are visually iterating to find what X and Y will give us an acceptable image; orig refers to the pixel value of the original image; and comp refers to the pixel value of the composite image. The n's and m's still index rows and columns of the image and indicate that this operation is done on all 4000 by 4000 pixels. The symbol V is the DN of a given pixel and a given image.

As an arbitrary assumption, now, we assume that our visual experimentation has found that the value of X= 0.025 and Y=0.6 are acceptable values when comparing the original image with the candidate distributable image. This is to say, the distributable image with the "extra noise" is acceptably close to the original in an aesthetic sense. Note that since our individual random images had a random rms noise value around 10 DN, and that adding approximately 16 of these images together will increase the composite noise to around 40 DN, the X multiplication value of 0.025 will bring the added rms noise back to around 1 DN, or half the amplitude of our innate noise on the original. This is roughly a 1 dB gain in noise at the dark pixel values and correspondingly more at the brighter values modified by the Y value of 0.6.

So with these two values of X and Y, we now have constructed our first versions of a distributable copy of the original. Other versions will merely create a new composite signal and possibly change the X slightly if deemed necessary. We now lock up the original digital image along with the 32-bit identification word for each version, and the 32 independent random 4-bit images, waiting for our first case of a suspected piracy of our original. Storage wise, this is about 14 Megabytes for the original image and 32*0.5bytes*16 million = ~256 Megabytes for the random individual encoded images. This is quite acceptable for a single valuable image. Some storage economy can be gained by simple lossless compression.

Finding a Suspected Piracy of our Image

We sell our image and several months later find our two heads of state in the exact poses we sold them in, seemingly cut and lifted out of our image and placed into another stylized background scene. This new "suspect" image is being printed in 100,000 copies of a given magazine issue, let us say. We now go about determining if a portion of our original image has indeed been used in an unauthorized manner. Fig. 3 summarizes the details.

The first step is to take an issue of the magazine, cut out the page with the image on it, then carefully but not too carefully cut out the two figures from the background image using ordinary scissors. If possible, we will cut out only one connected piece rather than the two figures separately. We paste this onto a black background and scan this into a digital form. Next we electronically flag or mask out the black background, which is easy to do by visual inspection.

We now procure the original digital image from our secured place along with the 32-bit identification word and the 32 individual embedded images. We place the original digital image onto our computer screen using standard image manipulation software, and we roughly cut along the same borders as our masked area of the suspect image, masking this image at the same time in roughly the same manner. The word 'roughly' is used since an exact cutting is not needed, it merely aids the identification statistics to get it reasonably close.

Next we rescale the masked suspect image to roughly match the size of our masked original digital image, that is, we digitally scale up or down the suspect image and roughly overlay it on the original image. Once we have performed this rough registration, we then throw the two images into an automated scaling and registration program. The program performs a search on the three parameters of x position, y position, and spatial scale, with the figure of merit being the mean squared error between the two images given any given scale variable and x and y offset. This is a fairly standard image processing methodology. Typically this would be done using generally smooth interpolation techniques and done to sub-pixel accuracy. The search method can be one of many, where the simplex method is a typical one.

Once the optimal scaling and x-y position variables are found, next comes another search on optimizing the black level, brightness gain, and gamma of the two images. Again, the figure of merit to be used is mean squared error, and again the simplex or other search methodologies can be used to optimize the three variables. After these three variables are optimized, we apply their corrections to the suspect image and align it to exactly the pixel spacing and masking of the original digital image and its mask. We can now call this the standard mask.

The next step is to subtract the original digital image from the newly normalized suspect image only within the standard mask region. This new image is called the difference image.

Then we step through all 32 individual random embedded images, doing a local cross-correlation between the masked difference image and the masked individual embedded image. 'Local' refers to the idea that one need only start correlating over an offset region of +/- 1 pixels of offset between the nominal registration points of the two images found during the search procedures above. The peak correlation should be very close to the nominal registration point of 0,0 offset, and we can add the 3 by 3 correlation values together to give one grand correlation value for each of the 32 individual bits of our 32-bit identification word.

After doing this for all 32 bit places and their corresponding random images, we have a quasi-floating point sequence of 32 values. The first four values represent our calibration signal of 0101. We now take the mean of the first and third floating point value and call this floating point value '0,' and we take the mean of the second and the fourth value and call this floating point value '1.' We then step through all remaining 28 bit values and assign either a '0' or a '1' based simply on which mean value they are closer to. Stated simply, if the suspect image is indeed a copy of our original, the embedded 32-bit

resulting code should match that of our records, and if it is not a copy, we should get general randomness. The third and the fourth possibilities of 3) Is a copy but doesn't match identification number and 4) isn't a copy but does match are, in the case of 3), possible if the signal to noise ratio of the process has plummeted, i.e. the 'suspect image' is truly a very poor copy of the original, and in the case of 4) is basically one chance in four billion since we were using a 32-bit identification number. If we are truly worried about 4), we can just have a second independent lab perform their own tests on a different issue of the same magazine. Finally, checking the error-check bits against what the values give is one final and possibly overkill check on the whole process. In situations where signal to noise is a possible problem, these error checking bits might be eliminated without too much harm.

Benefits

Now that a full description of the first embodiment has been described via a detailed example, it is appropriate to point out the rationale of some of the process steps and their benefits.

The ultimate benefits of the foregoing process are that obtaining an identification number is fully independent of the manners and methods of preparing the difference image. That is to say, the manners of preparing the difference image, such as cutting, registering, scaling, etcetera, cannot increase the odds of finding an identification number when none exists; it only helps the signal-to-noise ratio of the identification process when a true identification number is present. Methods of preparing images for identification can be different from each other even, providing the possibility for multiple independent methodologies for making a match.

The ability to obtain a match even on sub-sets of the original signal or image is a key point in today's information-rich world. Cutting and pasting both images and sound clips is becoming more common, allowing such an embodiment to be used in detecting a copy even when original material has been thus corrupted. Finally, the signal to noise ratio of matching should begin to become difficult only when the copy material itself has been significantly altered either by noise or by significant distortion; both of these also will affect that copy's commercial value, so that trying to thwart the system can only be done at the expense of a huge decrease in commercial value.

An early conception of this technology was the case where only a single "snowy image" or random signal was added to an original image, i.e. the case where $N=1$. "Decoding" this signal would involve a subsequent mathematical analysis using (generally statistical) algorithms to make a judgment on the presence or absence of this signal. The reason this approach was abandoned as the preferred embodiment was that there was an inherent gray area in the certainty of detecting the presence or absence of the signal. By moving onward to a multitude of bit planes, i.e. $N > 1$, combined with simple pre-defined algorithms prescribing the manner of choosing between a "0" and a "1", the certainty question moved from the realm of expert statistical analysis into the realm of guessing a random binary event such

as a coin flip. This is seen as a powerful feature relative to the intuitive acceptance of this technology in both the courtroom and the marketplace. The analogy which summarizes the inventor's thoughts on this whole question is as follows: The search for a single identification signal amounts to calling a coin flip only once, and relying on arcane experts to make the call; whereas the $N > 1$ embodiment relies on the broadly intuitive principle of correctly calling a coin flip N times in a row. This situation is greatly exacerbated, i.e. the problems of "interpretation" of the presence of a single signal, when images and sound clips get smaller and smaller in extent.

Another important reason that the $N > 1$ case is preferred over the $N = 1$ embodiment is that in the $N = 1$ case, the manner in which a suspect image is prepared and manipulated has a direct bearing on the likelihood of making a positive identification. Thus, the manner with which an expert makes an identification determination becomes an integral part of that determination. The existence of a multitude of mathematical and statistical approaches to making this determination leave open the possibility that some tests might make positive identifications while others might make negative determinations, inviting further arcane debate about the relative merits of the various identification approaches. The $N > 1$ embodiment avoids this further gray area by presenting a method where no amount of pre-processing of a signal - other than pre-processing which surreptitiously uses knowledge of the private code signals - can increase the likelihood of "calling the coin flip N times in a row."

The fullest expression of the present system will come when it becomes an industry standard and numerous independent groups set up with their own means or 'in-house' brand of applying embedded identification numbers and in their decipherment. Numerous independent group identification will further enhance the ultimate objectivity of the method, thereby enhancing its appeal as an industry standard.

Use of True Polarity in Creating the Composite Embedded Code Signal

The foregoing discussion made use of the 0 and 1 formalism of binary technology to accomplish its ends. Specifically, the 0's and 1's of the N-bit identification word directly multiplied their corresponding individual embedded code signal to form the composite embedded code signal (step 8, Fig. 2). This approach certainly has its conceptual simplicity, but the multiplication of an embedded code signal by 0 along with the storage of that embedded code contains a kind of inefficiency.

It is preferred to maintain the formalism of the 0 and 1 nature of the N-bit identification word, but to have the 0's of the word induce a subtraction of their corresponding embedded code signal. Thus, in step 8 of Fig. 2, rather than only 'adding' the individual embedded code signals which correspond to a '1' in the N-bit identification word, we will also 'subtract' the individual embedded code signals which correspond to a '0' in the N-bit identification word.

At first glance this seems to add more apparent noise to the final composite signal. But it also increases the energy-wise separation of the 0's from the 1's, and thus the 'gain' which is applied in step 10, Fig. 2 can be correspondingly lower.

We can refer to this improvement as the use of true polarity. The main advantage of this improvement can largely be summarized as 'informational efficiency.'

'Perceptual Orthogonality' of the Individual Embedded Code Signals

The foregoing discussion contemplates the use of generally random noise-like signals as the individual embedded code signals. This is perhaps the simplest form of signal to generate. However, there is a form of informational optimization which can be applied to the set of the individual embedded signals, which the applicant describes under the rubric 'perceptual orthogonality.' This term is loosely based on the mathematical concept of the orthogonality of vectors, with the current additional requirement that this orthogonality should maximize the signal energy of the identification information while maintaining it below some perceptibility threshold. Put another way, the embedded code signals need not necessarily be random in nature.

Use and Improvements of the First Embodiment in the Field of Emulsion-Based Photography

The foregoing discussion outlined techniques that are applicable to photographic materials. The following section explores the details of this area further and discloses certain improvements which lend themselves to a broad range of applications.

The first area to be discussed involves the pre-application or pre-exposing of a serial number onto traditional photographic products, such as negative film, print paper, transparencies, etc. In general, this is a way to embed *a priori* unique serial numbers (and by implication, ownership and tracking information) into photographic material. The serial numbers themselves would be a permanent part of the normally exposed picture, as opposed to being relegated to the margins or stamped on the back of a printed photograph, which all require separate locations and separate methods of copying. The 'serial number' as it is called here is generally synonymous with the N-bit identification word, only now we are using a more common industrial terminology.

In Fig. 2, step 11, the disclosure calls for the storage of the "original [image]" along with code images. Then in Fig. 3, step 9, it directs that the original be subtracted from the suspect image, thereby leaving the possible identification codes plus whatever noise and corruption has accumulated. Therefore, the previous disclosure made the tacit assumption that there exists an original without the composite embedded signals.

Now in the case of selling print paper and other duplication film products, this will still be the case, i.e., an "original" without the embedded codes will indeed exist and the basic methodology of the first embodiment can be employed. The original film serves perfectly well as an 'unencoded original.'

However, in the case where pre-exposed negative film is used, the composite embedded signal pre-exists on the original film and thus there will never be an "original" separate from the pre-embedded signal. It is this latter case, therefore, which will be examined a bit more closely, along with observations on how to best use the principles discussed above (the former cases adhering to the previously outlined methods).

The clearest point of departure for the case of pre-numbered negative film, i.e. negative film which has had each and every frame pre-exposed with a very faint and unique composite embedded signal, comes at step 9 of Fig. 3 as previously noted. There are certainly other differences as well, but they are mostly logistical in nature, such as how and when to embed the signals on the film, how to store the code numbers and serial number, etc. Obviously the pre-exposing of film would involve a major change to the general mass production process of creating and packaging film.

Fig. 4 has a schematic outlining one potential post-hoc mechanism for pre-exposing film. 'Post-hoc' refers to applying a process after the full common manufacturing process of film has already taken place. Eventually, economies of scale may dictate placing this pre-exposing process directly into the chain of manufacturing film. Depicted in Fig. 4 is what is commonly known as a film writing system. The computer, 106, displays the composite signal produced in step 8, Fig. 2, on its phosphor screen. A given frame of film is then exposed by imaging this phosphor screen, where the exposure level is generally very faint, i.e. generally imperceptible. Clearly, the marketplace will set its own demands on how faint this should be, that is, the level of added 'graininess' as practitioners would put it. Each frame of film is sequentially exposed, where in general the composite image displayed on the CRT 102 is changed for each and every frame, thereby giving each frame of film a different serial number. The transfer lens 104 highlights the focal conjugate planes of a film frame and the CRT face.

Getting back to the applying the principles of the foregoing embodiment in the case of pre-exposed negative film... At step 9, Fig. 3, if we were to subtract the "original" with its embedded code, we would obviously be "erasing" the code as well since the code is an integral part of the original. Fortunately, remedies do exist and identifications can still be made. However, it will be a challenge to artisans who refine this embodiment to have the signal to noise ratio of the identification process in the pre-exposed negative case approach the signal to noise ratio of the case where the un-encoded original exists.

A succinct definition of the problem is in order at this point. Given a suspect picture (signal), find the embedded identification code IF a code exists at al. The problem reduces to one of finding the amplitude of each and every individual embedded code signal within the suspect picture, not only within the context of noise and corruption as was previously explained, but now also within the context of the

coupling between a captured image and the codes. 'Coupling' here refers to the idea that the captured image "randomly biases" the cross-correlation.

So, bearing in mind this additional item of signal coupling, the identification process now estimates the signal amplitude of each and every individual embedded code signal (as opposed to taking the cross-correlation result of step 12, Fig. 3). If our identification signal exists in the suspect picture, the amplitudes thus found will split into a polarity with positive amplitudes being assigned a '1' and negative amplitudes being assigned a '0'. Our unique identification code manifests itself. If, on the other hand, no such identification code exists or it is someone else's code, then a random gaussian-like distribution of amplitudes is found with a random hash of values.

It remains to provide a few more details on how the amplitudes of the individual embedded codes are found. Again, fortunately, this exact problem has been treated in other technological applications. Besides, throw this problem and a little food into a crowded room of mathematicians and statisticians and surely a half dozen optimized methodologies will pop out after some reasonable period of time. It is a rather cleanly defined problem.

One specific example solution comes from the field of astronomical imaging. Here, it is a mature prior art to subtract out a "thermal noise frame" from a given CCD image of an object. Often, however, it is not precisely known what scaling factor to use in subtracting the thermal frame, and a search for the correct scaling factor is performed. This is precisely the task of this step of the present embodiment.

General practice merely performs a common search algorithm on the scaling factor, where a scaling factor is chosen and a new image is created according to:

$$\text{NEW IMAGE} = \text{ACQUIRED IMAGE} - \text{SCALE} * \text{THERMAL IMAGE} \qquad (4)$$

The new image is applied to the fast fourier transform routine and a scale factor is eventually found which minimizes the integrated high frequency content of the new image. This general type of search operation with its minimization of a particular quantity is exceedingly common. The scale factor thus found is the sought-for "amplitude." Refinements which are contemplated but not yet implemented are where the coupling of the higher derivatives of the acquired image and the embedded codes are estimated and removed from the calculated scale factor. In other words, certain bias effects from the coupling mentioned earlier are present and should be eventually accounted for and removed both through theoretical and empirical experimentation.

Use and Improvements in the Detection of Signal or Image Alteration

Apart from the basic need of identifying a signal or image as a whole, there is also a rather ubiquitous need to detect possible alterations to a signal or image. The following section describes how the foregoing embodiment, with certain modifications and improvements, can be used as a powerful tool in this area. The potential scenarios and applications of detecting alterations are innumerable.

To first summarize, assume that we have a given signal or image which has been positively identified using the basic methods outlined above. In other words, we know its N-bit identification word, its individual embedded code signals, and its composite embedded code. We can then fairly simply create a spatial map of the composite code's amplitude within our given signal or image. Furthermore, we can divide this amplitude map by the known composite code's spatial amplitude, giving a normalized map, i.e. a map which should fluctuate about some global mean value. By simple examination of this map, we can visually detect any areas which have been significantly altered wherein the value of the normalized amplitude dips below some statistically set threshold based purely on typical noise and corruption (error).

The details of implementing the creation of the amplitude map have a variety of choices. One is to perform the same procedure which is used to determine the signal amplitude as described above, only now we step and repeat the multiplication of any given area of the signal/image with a gaussian weight function centered about the area we are investigating.

Universal Versus Custom Codes

The disclosure thus far has outlined how each and every source signal has its own unique set of individual embedded code signals. This entails the storage of a significant amount of additional code information above and beyond the original, and many applications may merit some form of economizing.

One such approach to economizing is to have a given set of individual embedded code signals be common to a batch of source materials. For example, one thousand images can all utilize the same basic set of individual embedded code signals. The storage requirements of these codes then become a small fraction of the overall storage requirements of the source material.

Furthermore, some applications can utilize a universal set of individual embedded code signals, i.e., codes which remain the same for all instances of distributed material. This type of requirement would be seen by systems which wish to hide the N-bit identification word itself, yet have standardized equipment be able to read that word. This can be used in systems which make go/no go decisions at point-of-read locations. The potential drawback to this set-up is that the universal codes are more prone to be sleuthed or stolen; therefore they will not be as secure as the apparatus and methodology of the previously disclosed arrangement. Perhaps this is just the difference between 'high security' and 'air-tight security,' a distinction carrying little weight with the bulk of potential applications.

Use in Printing, Paper, Documents, Plastic Coated Identification Cards, and Other Material Where Global Embedded Codes Can Be Imprinted

The term 'signal' is often used narrowly to refer to digital data information, audio signals, images, etc. A broader interpretation of 'signal,' and the one more generally intended, includes any form of modulation of any material whatsoever. Thus, the micro-topology of a piece of common paper becomes

a 'signal' (e.g. it height as a function of x-y coordinates). The reflective properties of a flat piece of plastic (as a function of space also) becomes a signal. The point is that photographic emulsions, audio signals, and digitized information are not the only types of signals capable of utilizing the principles described herein.

As a case in point, a machine very much resembling a braille printing machine can be designed so as to imprint unique 'noise-like' indentations as outlined above. These indentations can be applied with a pressure which is much smaller than is typically applied in creating braille, to the point where the patterns are not noticed by a normal user of the paper. But by following the steps of the present disclosure and applying them via the mechanism of micro-indentations, a unique identification code can be placed onto any given sheet of paper, be it intended for everyday stationary purposes, or be it for important documents, legal tender, or other secured material.

The reading of the identification material in such an embodiment generally proceeds by merely reading the document optically at a variety of angles. This would become an inexpensive method for deducing the micro-topology of the paper surface. Certainly other forms of reading the topology of the paper are possible as well.

In the case of plastic encased material such as identification cards, e.g. driver's licenses, a similar braille-like impressions machine can be utilized to imprint unique identification codes. Subtle layers of photoreactive materials can also be embedded inside the plastic and 'exposed.'

It is clear that wherever a material exists which is capable of being modulated by 'noise-like' signals, that material is an appropriate carrier for unique identification codes and utilization of the principles disclosed herein. All that remains is the matter of economically applying the identification information and maintaining the signal level below an acceptability threshold which each and every application will define for itself.

REAL TIME ENCODER

While the first class of embodiments most commonly employs a standard microprocessor or computer to perform the encodation of an image or signal, it is possible to utilize a custom encodation device which may be faster than a typical Von Neuman-type processor. Such a system can be utilized with all manner of serial data streams.

Music and videotape recordings are examples of serial data streams -- data streams which are often pirated. It would assist enforcement efforts if authorized recordings were encoded with identification data so that pirated knock-offs could be traced to the original from which they were made.

Piracy is but one concern driving the need for applicant's technology. Another is authentication. Often it is important to confirm that a given set of data is really what it is purported to be (often several years after its generation).

To address these and other needs, the system 200 of Fig. 5 can be employed. System 200 can be thought of as an identification coding black box 202. The system 200 receives an input signal (sometimes termed the "master" or "unencoded" signal) and a code word, and produces (generally in real time) an identification-coded output signal. (Usually, the system provides key data for use in later decoding.)

The contents of the "black box" 202 can take various forms. An exemplary black box system is shown in Fig. 6 and includes a look-up table 204, a digital noise source 206, first and second scalers 208, 210, an adder/subtracter 212, a memory 214, and a register 216.

The input signal (which in the illustrated embodiment is an 8 - 20 bit data signal provided at a rate of one million samples per second, but which in other embodiments could be an analog signal if appropriate A/D and D/A conversion is provided) is applied from an input 218 to the address input 220 of the look-up table 204. For each input sample (i.e. look-up table address), the table provides a corresponding 8-bit digital output word. This output word is used as a scaling factor that is applied to one input of the first scaler 208.

The first scaler 208 has a second input, to which is applied an 8-bit digital noise signal from source 206. (In the illustrated embodiment, the noise source 206 comprises an analog noise source 222 and an analog-to-digital converter 224 although, again, other implementations can be used.) The noise source in the illustrated embodiment has a zero mean output value, with a full width half maximum (FWHM) of 50 - 100 digital numbers (e.g. from -75 to +75).

The first scaler 208 multiplies the two 8-bit words at its inputs (scale factor and noise) to produce -- for each sample of the system input signal -- a 16-bit output word. Since the noise signal has a zero mean value, the output of the first scaler likewise has a zero mean value.

The output of the first scaler 208 is applied to the input of the second scaler 210. The second scaler serves a global scaling function, establishing the absolute magnitude of the identification signal that will ultimately be embedded into the input data signal. The scaling factor is set through a scale control device 226 (which may take a number of forms, from a simple rheostat to a graphically implemented control in a graphical user interface), permitting this factor to be changed in accordance with the requirements of different applications. The second scaler 210 provides on its output line 228 a scaled noise signal. Each sample of this scaled noise signal is successively stored in the memory 214.

(In the illustrated embodiment, the output from the first scaler 208 may range between -1500 and +1500 (decimal), while the output from the second scaler 210 is in the low single digits, (such as between -2 and +2).)

Register 216 stores a multi-bit identification code word. In the illustrated embodiment this code word consists of 8 bits, although larger code words (up to hundreds of bits) are commonly used. These bits are referenced, one at a time, to control how the input signal is modulated with the scaled noise signal.

In particular, a pointer 230 is cycled sequentially through the bit positions of the code word in register 216 to provide a control bit of "0" or "1" to a control input 232 of the adder/subtracter 212. If, for a particular input signal sample, the control bit is a "1", the scaled noise signal sample on line 232 is added to the input signal sample. If the control bit is a "0", the scaled noise signal sample is subtracted from the input signal sample. The output 234 from the adder/subtracter 212 provides the black box's output signal.

The addition or subtraction of the scaled noise signal in accordance with the bits of the code word effects a modulation of the input signal that is generally imperceptible. However, with knowledge of the contents of the memory 214, a user can later decode the encoding, determining the code number used in the original encoding process. (Actually, use of memory 214 is optional, as explained below.)

It will be recognized that the encoded signal can be distributed in well known ways, including converted to printed image form, stored on magnetic media (floppy diskette, analog or DAT tape, etc.), CD-ROM, etc. etc.

Decoding

A variety of techniques can be used to determine the identification code with which a suspect signal has been encoded. Two are discussed below. The first is less preferable than the latter for most applications, but is discussed herein so that the reader may have a fuller context within which to understand the disclosed technology.

More particularly, the first decoding method is a difference method, relying on subtraction of corresponding samples of the original signal from the suspect signal to obtain difference samples, which are then examined (typically individually) for deterministic coding indicia (i.e. the stored noise data). This approach may thus be termed a "sample-based, deterministic" decoding technique.

The second decoding method does not make use of the original signal. Nor does it examine particular samples looking for predetermined noise characteristics. Rather, the statistics of the suspect signal (or a portion thereof) are considered in the aggregate and analyzed to discern the presence of identification coding that permeates the entire signal. The reference to permeation means the entire identification code can be discerned from a small fragment of the suspect signal. This latter approach may thus be termed a "holographic, statistical" decoding technique.

Both of these methods begin by registering the suspect signal to match the original. This entails scaling (e.g. in amplitude, duration, color balance, etc.), and sampling (or resampling) to restore the original sample rate. As in the earlier described embodiment, there are a variety of well understood techniques by which the operations associated with this registration function can be performed.

As noted, the first decoding approach proceeds by subtracting the original signal from the registered, suspect signal, leaving a difference signal. The polarity of successive difference signal samples

can then be compared with the polarities of the corresponding stored noise signal samples to determine the identification code. That is, if the polarity of the first difference signal sample matches that of the first noise signal sample, then the first bit of the identification code is a "1." (In such case, the polarity of the 9th, 17th, 25th, etc. samples should also all be positive.) If the polarity of the first difference signal sample is opposite that of the corresponding noise signal sample, then the first bit of the identification code is a "0."

By conducting the foregoing analysis with eight successive samples of the difference signal, the sequence of bits that comprise the original code word can be determined. If, as in the illustrated embodiment, pointer 230 stepped through the code word one bit at a time, beginning with the first bit, during encoding, then the first 8 samples of the difference signal can be analyzed to uniquely determine the value of the 8-bit code word.

In a noise-free world (speaking here of noise independent of that with which the identification coding is effected), the foregoing analysis would always yield the correct identification code. But a process that is only applicable in a noise-free world is of limited utility indeed.

(Further, accurate identification of signals in noise-free contexts can be handled in a variety of other, simpler ways: e.g. checksums; statistically improbable correspondence between suspect and original signals; etc.)

While noise-induced aberrations in decoding can be dealt with -- to some degree -- by analyzing large portions of the signal, such aberrations still place a practical ceiling on the confidence of the process. Further, the villain that must be confronted is not always as benign as random noise. Rather, it increasingly takes the form of human-caused corruption, distortion, manipulation, etc. In such cases, the desired degree of identification confidence can only be achieved by other approaches.

The illustrated embodiment (the "holographic, statistical" decoding technique) relies on recombining the suspect signal with certain noise data (typically the data stored in memory 214), and analyzing the entropy of the resulting signal. "Entropy" need not be understood in its most strict mathematical definition, it being merely the most concise word to describe randomness (noise, smoothness, snowiness, etc.).

Most serial data signals are not random. That is, one sample usually correlates -- to some degree -- with the adjacent samples. Noise, in contrast, typically is random. If a random signal (e.g. noise) is added to (or subtracted from) a non-random signal, the entropy of the resulting signal generally increases. That is, the resulting signal has more random variations than the original signal. This is the case with the encoded output signal produced by the present encoding process; it has more entropy than the original, unencoded signal.

If, in contrast, the addition of a random signal to (or subtraction from) a non-random signal reduces entropy, then something unusual is happening. It is this anomaly that the present decoding process uses to detect embedded identification coding.

To fully understand this entropy-based decoding method, it is first helpful to highlight a characteristic of the original encoding process: the similar treatment of every eighth sample.

In the encoding process discussed above, the pointer 230 increments through the code word, one bit for each successive sample of the input signal. If the code word is eight bits in length, then the pointer returns to the same bit position in the code word every eighth signal sample. If this bit is a "1", noise is added to the input signal; if this bit is a "0", noise is subtracted from the input signal. Due to the cyclic progression of the pointer 230, every eighth sample of an encoded signal thus shares a characteristic: they are all either augmented by the corresponding noise data (which may be negative), or they are all diminished, depending on whether the bit of the code word then being addressed by pointer 230 is a "1" or a "0".

To exploit this characteristic, the entropy-based decoding process treats every eighth sample of the suspect signal in like fashion. In particular, the process begins by adding to the 1st, 9th, 17th, 25th, etc. samples of the suspect signal the corresponding scaled noise signal values stored in the memory 214 (i.e. those stored in the 1st, 9th, 17th, 25th, etc., memory locations, respectively). The entropy of the resulting signal (i.e. the suspect signal with every 8th sample modified) is then computed.

(Computation of a signal's entropy or randomness is well understood by artisans in this field. One generally accepted technique is to take the derivative of the signal at each sample point, square these values, and then sum over the entire signal. However, a variety of other well known techniques can alternatively be used.)

The foregoing step is then repeated, this time subtracting the stored noise values from the 1st, 9th, 17th, 25 etc. suspect signal samples.

One of these two operations will undo the encoding process and reduce the resulting signal's entropy; the other will aggravate it. If adding the noise data in memory 214 to the suspect signal reduces its entropy, then this data must earlier have been subtracted from the original signal. This indicates that pointer 230 was pointing to a "0" bit when these samples were encoded. (A "0" at the control input of adder/subtracter 212 caused it to subtract the scaled noise from the input signal.)

Conversely, if subtracting the noise data from every eighth sample of the suspect signal reduces its entropy, then the encoding process must have earlier added this noise. This indicates that pointer 230 was pointing to a "1" bit when samples 1, 9, 17, 25, etc., were encoded.

By noting whether entropy decreases by (a) adding or (b) subtracting the stored noise data to/from the suspect signal, it can be determined that the first bit of the code word is (a) a "0", or (b) a "1".

The foregoing operations are then conducted for the group of spaced samples of the suspect signal beginning with the second sample (i.e. 2, 10, 18, 26 ...). The entropy of the resulting signals indicate whether the second bit of the code word is a "0" or a "1". Likewise with the following 6 groups of spaced samples in the suspect signal, until all 8 bits of the code word have been discerned.

It will be appreciated that the foregoing approach is not sensitive to corruption mechanisms that alter the values of individual samples; instead, the process considers the entropy of the signal as a whole, yielding a high degree of confidence in the results. Further, even small excerpts of the signal can be analyzed in this manner, permitting piracy of even small details of an original work to be detected. The results are thus statistically robust, both in the face of natural and human corruption of the suspect signal.

It will further be appreciated that the use of an N-bit code word in this real time embodiment provides benefits analogous to those discussed above in connection with the batch encoding system. (Indeed, the present embodiment may be conceptualized as making use of N different noise signals, just as in the batch encoding system. The first noise signal is a signal having the same extent as the input signal, and comprising the scaled noise signal at the 1st, 9th, 17th, 25th, etc., samples (assuming N=8), with zeroes at the intervening samples. The second noise signal is a similar one comprising the scaled noise signal at the 2d, 10th, 18th, 26th, etc., samples, with zeroes at the intervening samples. Etc. These signals are all combined to provide a composite noise signal.) One of the important advantages inherent in such a system is the high degree of statistical confidence (confidence which doubles with each successive bit of the identification code) that a match is really a match. The system does not rely on subjective evaluation of a suspect signal for a single, deterministic embedded code signal.

Illustrative Variations

From the foregoing description, it will be recognized that numerous modifications can be made to the illustrated systems without changing the fundamental principles. A few of these variations are described below.

The above-described decoding process tries both adding and subtracting stored noise data to/from the suspect signal in order to find which operation reduces entropy. In other embodiments, only one of these operations needs to be conducted. For example, in one alternative decoding process the stored noise data corresponding to every eighth sample of the suspect signal is only added to said samples. If the entropy of the resulting signal is thereby increased, then the corresponding bit of the code word is a "1" (i.e. this noise was added earlier, during the encoding process, so adding it again only compounds the signal's randomness). If the entropy of the resulting signal is thereby decreased, then the corresponding bit of the code word is a "0". A further test of entropy if the stored noise samples are subtracted is not required.

The statistical reliability of the identification process (coding and decoding) can be designed to exceed virtually any confidence threshold (e.g. 99.9%, 99.99%, 99.999%, etc. confidence) by appropriate selection of the global scaling factors, etc. Additional confidence in any given application (unnecessary in most applications) can be achieved by rechecking the decoding process.

One way to recheck the decoding process is to remove the stored noise data from the suspect signal in accordance with the bits of the discerned code word, yielding a "restored" signal (e.g. if the first bit of the code word is found to be "1," then the noise samples stored in the 1st, 9th, 17th, etc. locations of the memory 214 are subtracted from the corresponding samples of the suspect signal). The entropy of the restored signal is measured and used as a baseline in further measurements. Next, the process is repeated, this time removing the stored noise data from the suspect signal in accordance with a modified code word. The modified code word is the same as the discerned code word, except 1 bit is toggled (e.g. the first). The entropy of the resulting signal is determined, and compared with the baseline. If the toggling of the bit in the discerned code word resulted in increased entropy, then the accuracy of that bit of the discerned code word is confirmed. The process repeats, each time with a different bit of the discerned code word toggled, until all bits of the code word have been so checked. Each change should result in an increase in entropy compared to the baseline value.

The data stored in memory 214 is subject to a variety of alternatives. In the foregoing discussion, memory 214 contains the scaled noise data. In other embodiments, the unscaled noise data can be stored instead.

In still other embodiments, it can be desirable to store at least part of the input signal itself in memory 214. For example, the memory can allocate 8 signed bits to the noise sample, and 16 bits to store the most significant bits of an 18- or 20-bit audio signal sample. This has several benefits. One is that it simplifies registration of a "suspect" signal. Another is that, in the case of encoding an input signal which was already encoded, the data in memory 214 can be used to discern which of the encoding processes was performed first. That is, from the input signal data in memory 214 (albeit incomplete), it is generally possible to determine with which of two code words it has been encoded.

Yet another alternative for memory 214 is that is can be omitted altogether.

One way this can be achieved is to use a deterministic noise source in the encoding process, such as an algorithmic noise generator seeded with a known key number. The same deterministic noise source, seeded with the same key number, can be used in the decoding process. In such an arrangement, only the key number needs be stored for later use in decoding, instead of the large data set usually stored in memory 214.

Alternatively, if the noise signal added during encoding does not have a zero mean value, and the length N of the code word is known to the decoder, then a universal decoding process can be implemented. This process uses the same entropy test as the foregoing procedures, but cycles through possible code

words, adding/subtracting a small dummy noise value (e.g. less than the expected mean noise value) to every Nth sample of the suspect signal, in accordance with the bits of the code word being tested, until a reduction in entropy is noted. Such an approach is not favored for most applications, however, because it offers less security than the other embodiments (e.g. it is subject to cracking by brute force).

Many applications are well served by the embodiment illustrated in Fig. 7, in which different code words are used to produce several differently encoded versions of an input signal, each making use of the same noise data. More particularly, the embodiment 240 of Fig. 7 includes a noise store 242 into which noise from source 206 is written during the identification-coding of the input signal with a first code word. (The noise source of Fig. 7 is shown outside of the real time encoder 202 for convenience of illustration.) Thereafter, additional identification-coded versions of the input signal can be produced by reading the stored noise data from the store and using it in conjunction with second through Nth code words to encode the signal. (While binary-sequential code words are illustrated in Fig. 7, in other embodiments arbitrary sequences of code words can be employed.) With such an arrangement, a great number of differently-encoded signals can be produced, without requiring a proportionally-sized long term noise memory. Instead, a fixed amount of noise data is stored, whether encoding an original once or a thousand times.

(If desired, several differently-coded output signals can be produced at the same time, rather than seriatim. One such implementation includes a plurality of adder/subtracter circuits 212, each driven with the same input signal and with the same scaled noise signal, but with different code words. Each, then, produces a differently encoded output signal.)

In applications having a great number of differently-encoded versions of the same original, it will be recognized that the decoding process need not always discern every bit of the code word. Sometimes, for example, the application may require identifying only a group of codes to which the suspect signal belongs. (E.g., high order bits of the code word might indicate an organization to which several differently coded versions of the same source material were provided, with low-order bits identifying specific copies. To identify the organization with which a suspect signal is associated, it may not be necessary to examine the low order bits, since the organization can be identified by the high order bits alone.) If the identification requirements can be met by discerning a subset of the code word bits in the suspect signal, the decoding process can be shortened.

Some applications may be best served by restarting the encoding process -- sometimes with a different code word -- several times within an integral work. Consider, as an example, videotaped productions (e.g. television programming). Each frame of a videotaped production can be identification-coded with a unique code number, processed in real-time with an arrangement 248 like that shown in Fig. 8. Each time a vertical retrace is detected by sync detector 250, the noise source 206 resets (e.g. to repeat the sequence just produced) and an identification code increments to the next value. Each frame of the

videotape is thereby uniquely identification-coded. Typically, the encoded signal is stored on a videotape for long term storage (although other storage media, including laser disks, can be used).

Returning to the encoding apparatus, the look-up table 204 in the illustrated embodiment exploits the fact that high amplitude samples of the input data signal can tolerate (without objectionable degradation of the output signal) a higher level of encoded identification coding than can low amplitude input samples. Thus, for example, input data samples having decimal values of 0, 1 or 2 may be correspond (in the look-up table 204) to scale factors of unity (or even zero), whereas input data samples having values in excess of 200 may correspond to scale factors of 15. Generally speaking, the scale factors and the input sample values correspond by a square root relation. That is, a four-fold increase in a value of the sampled input signal corresponds to approximately a two-fold increase in a value of the scaling factor associated therewith.

(The parenthetical reference to zero as a scaling factor alludes to cases, e.g., in which the source signal is temporally or spatially devoid of information content. In an image, for example, a region characterized by several contiguous sample values of zero may correspond to a jet black region of the frame. A scaling value of zero may be appropriate here since there is essentially no image data to be pirated.)

Continuing with the encoding process, those skilled in the art will recognized the potential for "rail errors" in the illustrated embodiment. For example, if the input signal consists of 8-bit samples, and the samples span the entire range from 0 to 255 (decimal), then the addition or subtraction of scaled noise to/from the input signal may produce output signals that cannot be represented by 8 bits (e.g. -2, or 257). A number of well-understood techniques exist to rectify this situation, some of them proactive and some of them reactive. (Among these known techniques are: specifying that the input signal shall not have samples in the range of 0-4 or 251-255, thereby safely permitting modulation by the noise signal; or including provision for detecting and adaptively modifying input signal samples that would otherwise cause rail errors.)

While the illustrated embodiment describes stepping through the code word sequentially, one bit at a time, to control modulation of successive bits of the input signal, it will be appreciated that the bits of the code word can be used other than sequentially for this purpose. Indeed, bits of the code word can be selected in accordance with any predetermined algorithm.

The dynamic scaling of the noise signal based on the instantaneous value of the input signal is an optimization that can be omitted in many embodiments. That is, the look-up table 204 and the first scaler 208 can be omitted entirely, and the signal from the digital noise source 206 applied directly (or through the second, global scaler 210) to the adder/subtracter 212.

It will be further recognized that the use of a zero-mean noise source simplifies the illustrated embodiment, but is not essential. A noise signal with another mean value can readily be used, and D.C. compensation (if needed) can be effected elsewhere in the system.

The use of a noise source 206 is also optional. A variety of other signal sources can be used, depending on application- dependent constraints (e.g. the threshold at which the encoded identification signal becomes perceptible). In many instances, the level of the embedded identification signal is low enough that the identification signal needn't have a random aspect; it is imperceptible regardless of its nature. A pseudo random source 206, however, is usually desired because it provides the greatest identification code signal S/N ratio (a somewhat awkward term in this instance) for a level of imperceptibility of the embedded identification signal.

It will be recognized that identification coding need not occur after a signal has been reduced to stored form as data (i.e. "fixed in tangible form," in the words of the U.S. Copyright Act). Consider, for example, the case of popular musicians whose performances are often recorded illicitly. By identification coding the audio before it drives concert hall speakers, unauthorized recordings of the concert can be traced to a particular place and time. Likewise, live audio sources such as 911 emergency calls can be encoded prior to recording so as to facilitate their later authentication.

While the black box embodiment has been described as a stand alone unit, it will be recognized that it can be integrated into a number of different tools/instruments as a component. One is a scanner, which can embed identification codes in the scanned output data. (The codes can simply serve to memorialize that the data was generated by a particular scanner). Another is in creativity software, such as popular drawing/graphics/animation/paint programs offered by Adobe, Macromedia, Corel, and the like.

Finally, while the real-time encoder 202 has been illustrated with reference to a particular hardware implementation, it will be recognized that a variety of other implementations can alternatively be employed. Some utilize other hardware configurations. Others make use of software routines for some or all of the illustrated functional blocks. (The software routines can be executed on any number of different general purpose programmable computers, such as 80x86 PC-compatible computers, RISC-based workstations, etc.)

TYPES OF NOISE, QUASI-NOISE, AND OPTIMIZED-NOISE

Heretofore this disclosure postulated Gaussian noise, "white noise," and noise generated directly from application instrumentation as a few of the many examples of the kind of carrier signal appropriate to carry a single bit of information throughout an image or signal. It is possible to be even more proactive in "designing" characteristics of noise in order to achieve certain goals. The "design" of using Gaussian or instrumental noise was aimed somewhat toward "absolute" security. This section of the disclosure takes a

look at other considerations for the design of the noise signals which may be considered the ultimate carriers of the identification information.

For some applications it might be advantageous to design the noise carrier signal (e.g. the Nth embedded code signal in the first embodiment; the scaled noise data in the second embodiment), so as to provide more absolute signal strength to the identification signal relative to the perceptibility of that signal. One example is the following. It is recognized that a true Gaussian noise signal has the value '0' occur most frequently, followed by 1 and -1 at equal probabilities to each other but lower than '0', 2 and -2 next, and so on. Clearly, the value zero carries no information as it is used in such an embodiment. Thus, one simple adjustment, or design, would be that any time a zero occurs in the generation of the embedded code signal, a new process takes over, whereby the value is converted "randomly" to either a 1 or a -1. In logical terms, a decision would be made: if '0', then random(1,-1). The histogram of such a process would appear as a Gaussian/Poissonian type distribution, except that the 0 bin would be empty and the 1 and -1 bin would be increased by half the usual histogram value of the 0 bin.

In this case, identification signal energy would always be applied at all parts of the signal. A few of the trade-offs include: there is a (probably negligible) lowering of security of the codes in that a "deterministic component" is a part of generating the noise signal. The reason this might be completely negligible is that we still wind up with a coin flip type situation on randomly choosing the 1 or the -1. Another trade-off is that this type of designed noise will have a higher threshold of perceptibility, and will only be applicable to applications where the least significant bit of a data stream or image is already negligible relative to the commercial value of the material, i.e. if the least significant bit were stripped from the signal (for all signal samples), no one would know the difference and the value of the material would not suffer. This blocking of the zero value in the example above is but one of many ways to "optimize" the noise properties of the signal carrier, as anyone in the art can realize. We refer to this also as "quasi-noise" in the sense that natural noise can be transformed in a pre-determined way into signals which for all intents and purposes will read as noise. Also, cryptographic methods and algorithms can easily, and often by definition, create signals which are perceived as completely random. Thus the word "noise" can have different connotations, primarily between that as defined subjectively by an observer or listener, and that defined mathematically. The difference of the latter is that mathematical noise has different properties of security and the simplicity with which it can either be "sleuthed" or the simplicity with which instruments can "automatically recognize" the existence of this noise.

"Universal" Embedded Codes

The bulk of this disclosure teaches that for absolute security, the noise-like embedded code signals which carry the bits of information of the identification signal should be unique to each and every encoded signal, or, slightly less restrictive, that embedded code signals should be generated sparingly, such as using the

same embedded codes for a batch of 1000 pieces of film, for example. Be this as it may, there is a whole other approach to this issue wherein the use of what we will call "universal" embedded code signals can open up large new applications for this technology. The economics of these uses would be such that the de facto lowered security of these universal codes (e.g. they would be analyzable by time honored cryptographic decoding methods, and thus potentially thwarted or reversed) would be economically negligible relative to the economic gains that the intended uses would provide. Piracy and illegitimate uses would become merely a predictable "cost" and a source of uncollected revenue only; a simple line item in an economic analysis of the whole. A good analogy of this is in the cable industry and the scrambling of video signals. Everybody seems to know that crafty, skilled technical individuals, who may be generally law abiding citizens, can climb a ladder and flip a few wires in their cable junction box in order to get all the pay channels for free. The cable industry knows this and takes active measures to stop it and prosecute those caught, but the "lost revenue" derived from this practice remains prevalent but almost negligible as a percentage of profits gained from the scrambling system as a whole. The scrambling system as a whole is an economic success despite its lack of "absolute security."

The same holds true for applications of this technology wherein, for the price of lowering security by some amount, large economic opportunity presents itself. This section first describes what is meant by universal codes, then moves on to some of the interesting uses to which these codes can be applied.

Universal embedded codes generally refer to the idea that knowledge of the exact codes can be distributed. The embedded codes won't be put into a dark safe never to be touched until litigation arises (as alluded to in other parts of this disclosure), but instead will be distributed to various locations where on-the-spot analysis can take place. Generally this distribution will still take place within a security controlled environment, meaning that steps will be taken to limit the knowledge of the codes to those with a need to know. Instrumentation which attempts to automatically detect copyrighted material is a non-human example of "something" with a need to know the codes.

There are many ways to implement the idea of universal codes, each with their own merits regarding any given application. For the purposes of teaching this art, we separate these approaches into three broad categories: universal codes based on libraries, universal codes based on deterministic formula, and universal codes based on pre-defined industry standard patterns. A rough rule of thumb is that the first is more secure than the latter two, but that the latter two are possibly more economical to implement than the first.

Universal Codes: 1) Libraries of Universal Codes

The use of libraries of universal codes simply means that applicant's techniques are employed as described, except for the fact that only a limited set of the individual embedded code signals are generated and that any given encoded material will make use of some sub-set of this limited "universal set." An

example is in order here. A photographic print paper manufacturer may wish to pre-expose every piece of 8 by 10 inch print paper which they sell with a unique identification code. They also wish to sell identification code recognition software to their large customers, service bureaus, stock agencies, and individual photographers, so that all these people can not only verify that their own material is correctly marked, but so that they can also determine if third party material which they are about to acquire has been identified by this technology as being copyrighted. This latter information will help them verify copyright holders and avoid litigation, among many other benefits. In order to "economically" institute this plan, they realize that generating unique individual embedded codes for each and every piece of print paper would generate Terabytes of independent information, which would need storing and to which recognition software would need access. Instead, they decide to embed their print paper with 16 bit identification codes derived from a set of only 50 independent "universal" embedded code signals. The details of how this is done are in the next paragraph, but the point is that now their recognition software only needs to contain a limited set of embedded codes in their library of codes, typically on the order of 1 Megabyte to 10 Megabytes of information for 50x16 individual embedded codes splayed out onto an 8x10 photographic print (allowing for digital compression). The reason for picking 50 instead of just 16 is one of a little more added security, where if it were the same 16 embedded codes for all photographic sheets, not only would the serial number capability be limited to 2 to the 16th power, but lesser and lesser sophisticated pirates could crack the codes and remove them using software tools.

There are many different ways to implement this scheme, where the following is but one exemplary method. It is determined by the wisdom of company management that a 300 pixels per inch criteria for the embedded code signals is sufficient resolution for most applications. This means that a composite embedded code image will contain 3000 pixels by 2400 pixels to be exposed at a very low level onto each 8x10 sheet. This gives 7.2 million pixels. Using our staggered coding system such as described in the black box implementation of Figs. 5 and 6, each individual embedded code signal will contain only 7.2 million divided by 16, or approximately 450K true information carrying pixels, i.e. every 16th pixel along a given raster line. These values will typically be in the range of 2 to -2 in digital numbers, or adequately described by a signed 3 bit number. The raw information content of an embedded code is then approximately 3/8th's bytes times 450K or about 170 Kilobytes. Digital compression can reduce this further. All of these decisions are subject to standard engineering optimization principles as defined by any given application at hand, as is well known in the art. Thus we find that 50 of these independent embedded codes will amount to a few Megabytes. This is quite reasonable level to distribute as a "library" of universal codes within the recognition software. Advanced standard encryption devices could be employed to mask the exact nature of these codes if one were concerned that would-be pirates would buy the recognition software merely to reverse engineer the universal embedded codes. The recognition

software could simply unencrypt the codes prior to applying the recognition techniques taught in this disclosure.

The recognition software itself would certainly have a variety of features, but the core task it would perform is determining if there is some universal copyright code within a given image. The key questions become WHICH 16 of the total 50 universal codes it might contain, if any, and if there are 16 found, what are their bit values. The key variables in determining the answers to these questions are: registration, rotation, magnification (scale), and extent. In the most general case with no helpful hints whatsoever, all variables must be independently varied across all mutual combinations, and each of the 50 universal codes must then be checked by adding and subtracting to see if an entropy decrease occurs. Strictly speaking, this is an enormous job, but many helpful hints will be found which make the job much simpler, such as having an original image to compare to the suspected copy, or knowing the general orientation and extent of the image relative to an 8x10 print paper, which then through simple registration techniques can determine all of the variables to some acceptable degree. Then it merely requires cycling through the 50 universal codes to find any decrease in entropy. If one does, then 15 others should as well. A protocol needs to be set up whereby a given order of the 50 translates into a sequence of most significant bit through least significant bit of the ID code word. Thus if we find that universal code number "4" is present, and we find its bit value to be "0", and that universal codes "1" through "3" are definitely not present, then our most significant bit of our N-bit ID code number is a "0". Likewise, we find that the next lowest universal code present is number "7" and it turns out to be a "1", then our next most significant bit is a "1". Done properly, this system can cleanly trace back to the copyright owner so long as they registered their photographic paper stock serial number with some registry or with the manufacturer of the paper itself. That is, we look up in the registry that a paper using universal embedded codes 4,7,11,12,15,19,21,26,27,28,34,35,37,38,40, and 48, and having the embedded code 0110 0101 0111 0100 belongs to Leonardo de Boticelli, an unknown wildlife photographer and glacier cinematographer whose address is in Northern Canada. We know this because he dutifully registered his film and paper stock, a few minutes of work when he bought the stock, which he plopped into the "no postage necessary" envelope that the manufacturing company kindly provided to make the process ridiculously simple. Somebody owes Leonardo a royalty check it would appear, and certainly the registry has automated this royalty payment process as part of its services.

One final point is that truly sophisticated pirates and others with illicit intentions can indeed employ a variety of cryptographic and not so cryptographic methods to crack these universal codes, sell them, and make software and hardware tools which can assist in the removing or distorting of codes. We shall not teach these methods as part of this disclosure, however. In any event, this is one of the prices which must be paid for the ease of universal codes and the applications they open up.

Universal Codes: 2) Universal Codes Based on Deterministic Formulas

The libraries of universal codes require the storage and transmittal of Megabytes of independent, generally random data as the keys with which to unlock the existence and identity of signals and imagery that have been marked with universal codes. Alternatively, various deterministic formulas can be used which "generate" what appear to be random data/image frames, thereby obviating the need to store all of these codes in memory and interrogate each and of the "50" universal codes. Deterministic formulas can also assist in speeding up the process of determining the ID code once one is known to exist in a given signal or image. On the other hand, deterministic formulas lend themselves to sleuthing by less sophisticated pirates. And once sleuthed, they lend themselves to easier communication, such as posting on the Internet to a hundred newsgroups. There may well be many applications which do not care about sleuthing and publishing, and deterministic formulas for generating the individual universal embedded codes might be just the ticket.

Universal Codes: 3) "Simple" Universal Codes

This category is a bit of a hybrid of the first two, and is most directed at truly large scale implementations of the principles of this technology. The applications employing this class are of the type where staunch security is much less important than low cost, large scale implementation and the vastly larger economic benefits that this enables. One exemplary application is placement of identification recognition units directly within modestly priced home audio and video instrumentation (such as a TV). Such recognition units would typically monitor audio and/or video looking for these copyright identification codes, and thence triggering simple decisions based on the findings, such as disabling or enabling recording capabilities, or incrementing program specific billing meters which are transmitted back to a central audio/video service provider and placed onto monthly invoices. Likewise, it can be foreseen that "black boxes" in bars and other public places can monitor (listen with a microphone) for copyrighted materials and generate detailed reports, for use by ASCAP, BMI, and the like.

A core principle of simple universal codes is that some basic industry standard "noiselike" and seamlessly repetitive patterns are injected into signals, images, and image sequences so that inexpensive recognition units can either A) determine the mere existence of a copyright "flag", and B) additionally to A, determine precise identification information which can facilitate more complex decision making and actions.

In order to implement this particular embodiment, the basic principles of generating the individual embedded noise signals need to be simplified in order to accommodate inexpensive recognition signal processing circuitry, while maintaining the properties of effective randomness and holographic permeation. With large scale industry adoption of these simple codes, the codes themselves would border on public domain information (much as cable scrambling boxes are almost de facto public domain), leaving the door

open for determined pirates to develop black market countermeasures, but this situation would be quite analogous to the scrambling of cable video and the objective economic analysis of such illegal activity.

One prior art known to the applicant in this general area of pro-active copyright detection is the Serial Copy Management System adopted by many firms in the audio industry. To the best of applicant's knowledge, this system employs a non-audio "flag" signal which is not part of the audio data stream, but which is nevertheless grafted onto the audio stream and can indicate whether the associated audio data should or should not be duplicated. One problem with this system is that it is restricted to media and instrumentation which can support this extra "flag" signal. Another deficiency is that the flagging system carries no identity information which would be useful in making more complex decisions. Yet another difficulty is that high quality audio sampling of an analog signal can come arbitrarily close to making a perfect digital copy of some digital master and there seems to be no provision for inhibiting this possibility.

Applicant's technology can be brought to bear on these and other problems, in audio applications, video, and all of the other applications previously discussed. An exemplary application of simple universal codes is the following. A single industry standard "1.000000 second of noise" would be defined as the most basic indicator of the presence or absence of the copyright marking of any given audio signal. Fig. 9 has an example of what the waveform of an industry standard noise second might look like, both in the time domain 400 and the frequency domain 402. It is by definition a continuous function and would adapt to any combination of sampling rates and bit quantizations. It has a normalized amplitude and can be scaled arbitrarily to any digital signal amplitude. The signal level and the first M'th derivatives of the signal are continuous at the two boundaries 404 (Fig. 9C), such that when it is repeated, the "break" in the signal would not be visible (as a waveform) or audible when played through a high end audio system. The choice of 1 second is arbitrary in this example, where the precise length of the interval will be derived from considerations such as audibility, quasi-white noise status, seamless repeatability, simplicity of recognition processing, and speed with which a copyright marking determination can be made. The injection of this repeated noise signal onto a signal or image (again, at levels below human perception) would indicate the presence of copyright material. This is essentially a one bit identification code, and the embedding of further identification information will be discussed later on in this section. The use of this identification technique can extend far beyond the low cost home implementations discussed here, where studios could use the technique, and monitoring stations could be set up which literally monitor hundreds of channels of information simultaneously, searching for marked data streams, and furthermore searching for the associated identity codes which could be tied in with billing networks and royalty tracking systems.

This basic, standardized noise signature is seamlessly repeated over and over again and added to audio signals which are to be marked with the base copyright identification. Part of the reason for the word "simple" is seen here: clearly pirates will know about this industry standard signal, but their illicit

uses derived from this knowledge, such as erasure or corruption, will be economically minuscule relative to the economic value of the overall technique to the mass market. For most high end audio this signal will be some 80 to 100 dB down from full scale, or even much further; each situation can choose its own levels though certainly there will be recommendations. The amplitude of the signal can be modulated according to the audio signal levels to which the noise signature is being applied, i.e. the amplitude can increase significantly when a drum beats, but not so dramatically as to become audible or objectionable. These measures merely assist the recognition circuitry to be described.

Recognition of the presence of this noise signature by low cost instrumentation can be effected in a variety of ways. One rests on basic modifications to the simple principles of audio signal power metering. Software recognition programs can also be written, and more sophisticated mathematical detection algorithms can be applied to audio in order to make higher confidence detection identifications. In such embodiments, detection of the copyright noise signature involves comparing the time averaged power level of an audio signal with the time averaged power level of that same audio signal which has had the noise signature subtracted from it. If the audio signal with the noise signature subtracted has a lower power level that the unchanged audio signal, then the copyright signature is present and some status flag to that effect needs to be set. The main engineering subtleties involved in making this comparison include: dealing with audio speed playback discrepancies (e.g. an instrument might be 0.5% "slow" relative to exactly one second intervals); and, dealing with the unknown phase of the one second noise signature within any given audio (basically, its "phase" can be anywhere from 0 to 1 seconds). Another subtlety, not so central as the above two but which nonetheless should be addressed, is that the recognition circuits should not subtract a higher amplitude of the noise signature than was originally embedded onto the audio signal. Fortunately this can be accomplished by merely subtracting only a small amplitude of the noise signal, and if the power level goes down, this is an indication of "heading toward a trough" in the power levels. Yet another related subtlety is that the power level changes will be very small relative to the overall power levels, and calculations generally will need to be done with appropriate bit precision, e.g. 32 bit value operations and accumulations on 16-20 bit audio in the calculations of time averaged power levels.

Clearly, designing and packaging this power level comparison processing circuitry for low cost applications is an engineering optimization task. One trade-off will be the accuracy of making an identification relative to the "short-cuts" which can be made to the circuitry in order to lower its cost and complexity. One embodiment for placing this recognition circuitry inside of instrumentation is through a single programmable integrated circuit which is custom made for the task. Fig. 10 shows one such integrated circuit 506. Here the audio signal comes in, 500, either as a digital signal or as an analog signal to be digitized inside the IC 500, and the output is a flag 502 which is set to one level if the copyright noise signature is found, and to another level if it is not found. Also depicted is the fact that the

standardized noise signature waveform is stored in Read Only Memory, 504, inside the IC 506. There will be a slight time delay between the application of an audio signal to the IC 506 and the output of a valid flag 502, due to the need to monitor some finite portion of the audio before a recognition can place. In this case, there may need to be a "flag valid" output 508 where the IC informs the external world if it has had enough time to make a proper determination of the presence or absence of the copyright noise signature.

There are a wide variety of specific designs and philosophies of designs applied to accomplishing the basic function of the IC 506 of Fig. 10. Audio engineers and digital signal processing engineers are able to generate several fundamentally different designs. One such design is depicted in Fig. 11 by a process 599, which itself is subject to further engineering optimization as will be discussed. Fig. 11 depicts a flow chart for any of: an analog signal processing network, a digital signal processing network, or programming steps in a software program. We find an input signal 600 which along one path is applied to a time averaged power meter 602, and the resulting power output itself treated as a signal P_{sig}. To the upper right we find the standard noise signature 504 which will be read out at 125% of normal speed, 604, thus changing its pitch, giving the "pitch changed noise signal" 606. Then the input signal has this pitch changed noise signal subtracted in step 608, and this new signal is applied to the same form of time averaged power meter as in 602, here labelled 610. The output of this operation is also a time based signal here labelled as P_{s-pcn}, 610. Step 612 then subtracts the power signal 602 from the power signal 610, giving an output difference signal P_{out}, 613. If the universal standard noise signature does indeed exist on the input audio signal 600, then case 2, 616, will be created wherein a beat signal 618 of approximately 4 second period will show up on the output signal 613, and it remains to detect this beat signal with a step such as in Fig. 12, 622. Case 1, 614, is a steady noisy signal which exhibits no periodic beating. 125% at step 604 is chosen arbitrarily here, where engineering considerations would determine an optimal value, leading to different beat signal frequencies 618. Whereas waiting 4 seconds in this example would be quite a while, especially is you would want to detect at least two or three beats, Fig. 12 outlines how the basic design of Fig. 11 could be repeated and operated upon various delayed versions of the input signal, delayed by something like 1/20th of a second, with 20 parallel circuits working in concert each on a segment of the audio delayed by 0.05 seconds from their neighbors. In this way, a beat signal will show up approximately every 1/5th of a second and will look like a travelling wave down the columns of beat detection circuits. The existence or absence of this travelling beat wave triggers the detection flag 502. Meanwhile, there would be an audio signal monitor 624 which would ensure that, for example, at least two seconds of audio has been heard before setting the flag valid signal 508.

Though the audio example was described above, it should be clear to anyone in the art that the same type of definition of some repetitive universal noise signal or image could be applied to the many other signals, images, pictures, and physical media already discussed.

The above case deals only with a single bit plane of information, i.e., the noise signature signal is either there (1) or it isn't (0). For many applications, it would be nice to detect serial number information as well, which could then be used for more complex decisions, or for logging information on billing statements or whatnot. The same principles as the above would apply, but now there would be N independent noise signatures as depicted in Fig. 9 instead one single such signature. Typically, one such signature would be the master upon which the mere existence of a copyright marking is detected, and this would have generally higher power than the others, and then the other lower power "identification" noise signatures would be embedded into audio. Recognition circuits, once having found the existence of the primary noise signature, would then step through the other N noise signatures applying the same steps as described above. Where a beat signal is detected, this indicates the bit value of '1', and where no beat signal is detected, this indicates a bit value of '0'. It might be typical that N will equal 32, that way 2^{32} number of identification codes are available to any given industry employing this technology.

Use of this Technology When the Length of the Identification Code is 1

The principles described herein can obviously be applied in the case where only a single presence or absence of an identification signal -- a fingerprint if you will -- is used to provide confidence that some signal or image is copyrighted. The example above of the industry standard noise signature is one case in point. We no longer have the added confidence of the coin flip analogy, we no longer have tracking code capabilities or basic serial number capabilities, but many applications may not require these attributes and the added simplicity of a single fingerprint might outweigh these other attributes in any event.

The "Wallpaper" Analogy

The term "holographic" has been used in this disclosure to describe how an identification code number is distributed in a largely integral form throughout an encoded signal or image. This also refers to the idea that any given fragment of the signal or image contains the entire unique identification code number. As with physical implementations of holography, there are limitations on how small a fragment can become before one begins to lose this property, where the resolution limits of the holographic media are the main factor in this regard for holography itself. In the case of an uncorrupted distribution signal which has used the encoding device of Fig. 5, and which furthermore has used our "designed noise" of above wherein the zero's were randomly changed to a 1 or -1, then the extent of the fragment required is merely N contiguous samples in a signal or image raster line, where N is as defined previously being the length of our identification code number. This is an informational extreme; practical situations where noise and corruption are operative will require generally one, two or higher orders of magnitude more samples than this simple number N. Those skilled in the art will recognize that there are many variables

involved in pinning down precise statistics on the size of the smallest fragment with which an identification can be made.

For tutorial purposes, the applicant also uses the analogy that the unique identification code number is "wallpapered" across and image (or signal). That is, it is repeated over and over again all throughout an image. This repetition of the ID code number can be regular, as in the use of the encoder of Fig. 5, or random itself, where the bits in the ID code 216 of Fig. 6 are not stepped through in a normal repetitive fashion but rather are randomly selected on each sample, and the random selection stored along with the value of the output 228 itself. in any event, the information carrier of the ID code, the individual embedded code signal, does change across the image or signal. Thus as the wallpaper analogy summarizes: the ID code repeats itself over and over, but the patterns that each repetition imprints change randomly accordingly to a generally unsleuthable key.

Lossy Data Compression

As earlier mentioned, applicant's preferred forms of identification coding withstand lossy data compression, and subsequent decompression. Such compression is finding increasing use, particularly in contexts such as the mass distribution of digitized entertainment programming (movies, etc.).

While data encoded according to the disclosed techniques can withstand all types of lossy compression known to applicant, those expected to be most commercially important are the CCITT G3, CCITT G4, JPEG, MPEG and JBIG compression/decompression standards. The CCITT standards are widely used in black-and-white document compression (e.g. facsimile and document-storage). JPEG is most widely used with still images. MPEG is most widely used with moving images. JBIG is a likely successor to the CCITT standards for use with black-and-white imagery. Such techniques are well known to those in the lossy data compression field; a good overview can be found in Pennebaker et al, *JPEG, Still Image Data Compression Standard*, Van Nostrand Reinhold, N.Y., 1993.

Towards Steganography Proper and the Use of this Technology in Passing More Complex Messages or Information

This disclosure concentrates on what above was called wallpapering a single identification code across an entire signal. This appears to be a desirable feature for many applications. However, there are other applications where it might be desirable to pass messages or to embed very long strings of pertinent identification information in signals and images. One of many such possible applications would be where a given signal or image is meant to be manipulated by several different groups, and that certain regions of an image are reserved for each group's identification and insertion of pertinent manipulation information.

In these cases, the code word 216 in Fig. 6 can actually change in some pre-defined manner as a function of signal or image position. For example, in an image, the code could change for each and every

raster line of the digital image. It might be a 16 bit code word, 216, but each scan line would have a new code word, and thus a 480 scan line image could pass a 980 (480 x 2 bytes) byte message. A receiver of the message would need to have access to either the noise signal stored in memory 214, or would have to know the universal code structure of the noise codes if that method of coding was being used. To the best of applicant's knowledge, this is a novel approach to the mature field of steganography.

In all three of the foregoing applications of universal codes, it will often be desirable to append a short (perhaps 8- or 16-bit) private code, which users would keep in their own secured places, in addition to the universal code. This affords the user a further modicum of security against potential erasure of the universal codes by sophisticated pirates.

Applicant's Prior Application

The Detailed Description to this point has simply repeated the disclosure of applicant's prior international application, laid open as PCT publication WO 95/14289. It was reproduced above simply to provide context for the disclosure which follows.

One Master Code Signal As A Distinction From N Independent Embedded Code Signals

In certain sections of this disclosure, perhaps exemplified in the section on the realtime encoder, an economizing step was taken whereby the N independent and source-signal-coextensive embedded code signals were so designed that the non-zero elements of any given embedded code signal were unique to just that embedded code signal and no others. Said more carefully, certain pixels/sample points of a given signal were "assigned" to some pre-determined m'th bit location in our N-bit identification word. Furthermore, and as another basic optimization of implementation, the aggregate of these assigned pixels/samples across all N embedded code signals is precisely the extent of the source signal, meaning each and every pixel/sample location in a source signal is assigned one and only one m'th bit place in our N-bit identification word. (This is not to say, however, that each and every pixel MUST be modified). As a matter of simplification we can then talk about a single master code signal (or "Snowy Image") rather than N independent signals, realizing that pre-defined locations in this master signal correspond to unique bit locations in our N-bit identification word. We therefore construct, via this circuitous route, this rather simple concept on the single master noise signal. Beyond mere economization and simplification, there are also performance reasons for this shift, primarily derived from the idea that individual bit places in our N-bit identification word are no longer "competing" for the information carrying capacity of a single pixel/sample.

With this single master more clearly understood, we can gain new insights into other sections of this disclosure and explore further details within the given application areas.

More of Deterministic Universal Codes Using the Master Code Concept

One case in point is to further explore the use of Deterministic Universal Codes, labelled as item "2" in the sections devoted to universal codes. A given user of this technology may opt for the following variant use of the principles of this technology. The user in question might be a mass distributor of home videos, but clearly the principles would extend to all other potential users of this technology. Fig. 13 pictorially represents the steps involved. In the example the user is one "Alien Productions." They first create an image canvas which is coextensive to the size of the video frames of their movie "Bud's Adventures." On this canvas they print the name of the movie, they place their logo and company name. Furthermore, they have specific information at the bottom, such as the distribution lot for the mass copying that they are currently cranking out, and as indicated, they actually have a unique frame number indicated. Thus we find the example of a standard image 700 which forms the initial basis for the creation of a master Snowy Image (master code signal) which will be added into the original movie frame, creating an output distributable frame. This image 700 can be either black & white or color. The process of turning this image 700 into a pseudo random master code signal is alluded to by the encryption/scrambling routine 702, wherein the original image 700 is passed through any of dozens of well known scrambling methods. The depiction of the number "28" alludes to the idea that there can actually be a library of scrambling methods, and the particular method used for this particular movie, or even for this particular frame, can change. The result is our classic master code signal or Snowy Image. In general, its brightness values are large and it would look very much like the snowy image on a television set tuned to a blank channel, but clearly it has been derived from an informative image 700, transformed through a scrambling 702. (Note: the splotchiness of the example picture is actually a rather poor depiction; it was a function of the crude tools available to the inventor).

This Master Snowy Image 704 is then the signal which is modulated by our N-bit identification word as outlined in other sections of the disclosure, the resulting modulated signal is then scaled down in brightness to the acceptable perceived noise level, and then added to the original frame to produce the distributable frame.

There are a variety of advantages and features that the method depicted in Fig. 13 affords. There are also variations of theme within this overall variation. Clearly, one advantage is that users can now use more intuitive and personalized methods for stamping and signing their work. Provided that the encryption/scrambling routines, 702, are indeed of a high security and not published or leaked, then even if a would-be pirate has knowledge of the logo image 700, they should not be able to use this knowledge to be able to sleuth the Master Snowy Image 704, and thus they should not be able to crack the system, as it were. On the other hand, simple encryption routines 702 may open the door for cracking the system. Another clear advantage of the method of Fig. 13 is the ability to place further information into the overall protective process. Strictly speaking, the information contained in the logo image 700 is not directly

carried in the final distributable frame. Said another way, and provided that the encryption/scrambling routine 702 has a straightforward and known decryption/descrambling method which tolerates bit truncation errors, it is generally impossible to fully re-create the image 700 based upon having the distributable frame, the N-bit identification code word, the brightness scaling factor used, and the number of the decryption routine to be used. The reason that an exact recreation of the image 700 is impossible is due to the scaling operation itself and the concomitant bit truncation. For the present discussion, this whole issue is somewhat academic, however.

A variation on the theme of Fig. 13 is to actually place the N-bit identification code word directly into the logo image 700. In some sense this would be self-referential. Thus when we pull out our stored logo image 700 it already contains visually what our identification word is, then we apply encryption routine #28 to this image, scale it down, then use this version to decode a suspect image using the techniques of this disclosure. The N bit word thus found should match the one contained in our logo image 700.

One desirable feature of the encryption/scrambling routine 702 might be (but is certainly not required to be) that even given a small change in the input image 700, such as a single digit change of the frame number, there would be a huge visual change in the output scrambled master snowy image 704. Likewise, the actual scrambling routine may change as a function of frame numbers, or certain "seed" numbers typically used within pseudo-randomizing functions could change as a function of frame number. All manner of variations are thus possible, all helping to maintain high levels of security. Eventually, engineering optimization considerations will begin to investigate the relationship between some of these randomizing methods, and how they all relate to maintaining acceptable signal strength levels through the process of transforming an uncompressed video stream into a compressed video stream such as with the MPEG compression methodologies.

Another desired feature of the encryption process 702 is that it should be informationally efficient, i.e., that given any random input, it should be able to output an essentially spatially uniform noisy image with little to no residual spatial patterns beyond pure randomness. Any residual correlated patterns will contribute to inefficiency of encoding the N-bit identification word, as well as opening up further tools to would-be pirates to break the system.

Another feature of the method of Fig. 13 is that there is more intuitional appeal to using recognizable symbols as part of a decoding system, which should then translate favorably in the essentially lay environment of a courtroom. It strengthens the simplicity of the coin flip vernacular mentioned elsewhere. Jury members or judges will better relate to an owner's logo as being a piece of the key of recognizing a suspect copy as being a knock-off.

It should also be mentioned that, strictly speaking, the logo image 700 does not need to be randomized. The steps could equally apply straight to the logo image 700 directly. It is not entirely clear

to the inventor what practical goal this might have. A trivial extension of this concept to the case where N = 1 is where, simply and easily, the logo image 700 is merely added to an original image at a very low brightness level. The inventor does not presume this trivial case to be at all a novelty. In many ways this is similar to the age old issue of subliminal advertising, where the low light level patterns added to an image are recognizable to the human eye/brain system and - supposedly - operating on the human brain at an unconscious level. By pointing out these trivial extensions of the current technology, hopefully there can arise further clarity which distinguishes applicant's novel principles in relation to such well known prior art techniques.

5-bit Abridged Alphanumeric Code Sets and Others

It is desirable in some applications for the N-bit identification word to actually signify names, companies, strange words, messages, and the like. Most of this disclosure focuses on using the N-bit identification word merely for high statistical security, indexed tracking codes, and other index based message carrying. The information carrying capacity of "invisible signatures" inside imagery and audio is somewhat limited, however, and thus it would be wise to use our N bits efficiently if we actually want to "spell out" alphanumeric items in the N-bit identification word.

One way to do this is to define, or to use an already existing, reduced bit (e.g. less than 8-bit ASCII) standardized codes for passing alphanumeric messages. This can help to satisfy this need on the part of some applications. For example, a simple alphanumeric code could be built on a 5-bit index table, where for example the letters V,X,Q, and Z are not included, but the digits 0 through 9 are included. In this way, a 100 bit identification word could carry with it 20 alphanumeric symbols. Another alternative is to use variable bit length codes such as the ones used in text compression routines (e.g. Huffman) whereby more frequently used symbols have shorter bit length codes and less frequently used symbols have longer bit lengths.

More on Detecting and Recognizing the N-bit Identification Word in Suspect Signals

Classically speaking, the detection of the N-bit identification word fits nicely into the old art of detecting known signals in noise. Noise in this last statement can be interpreted very broadly, even to the point where an image or audio track itself can be considered noise, relative to the need to detect the underlying signature signals. One of many references to this older art is the book Kassam, Saleem A., "Signal Detection in Non-Gaussian Noise," Springer-Verlag, 1988 (generally available at well stocked libraries, e.g. available at the U.S. Library of Congress by catalog number TK5102.5 .K357 1988.

To the best of this inventor's current understanding, none of the material

in this book is directly applicable to the issue of discovering the polarity of applicant's embedded signals, but the broader principles are indeed applicable.

In particular, section 1.2 "Basic Concepts of Hypothesis Testing" of Kassam's book lays out the basic concept of a binary hypothesis, assigning the value "1" to one hypothesis and the value "0" to the other hypothesis. The last paragraph of that section is also on point regarding the earlier-described embodiment, i.e., that the "0" hypothesis corresponds to "noise only" case, whereas the "1" corresponds to the presence of a signal in the observations. Applicant's use of true polarity is not like this, however, where now the "0" corresponds to the presence of an inverted signal rather than to "noise-only." Also in the present embodiment, the case of "noise-only" is effectively ignored, and that an identification process will either come up with our N-bit identification word or it will come up with "garbage."

The continued and inevitable engineering improvement in the detection of embedded code signals will undoubtedly borrow heavily from this generic field of known signal detection. A common and well-known technique in this field is the so-called "matched filter," which is incidentally discussed early in section 2 of the Kassam book. Many basic texts on signal processing include discussions on this method of signal detection. This is also known in some fields as correlation detection. Furthermore, when the phase or location of a known signal is known a priori, such as is often the case in applications of this technology, then the matched filter can often be reduced to a simple vector dot product between a suspect image and the embedded signal associated with an m'th bit plane in our N-bit identification word. This then represents yet another simple "detection algorithm" for taking a suspect image and producing a sequence of 1s and 0s with the intention of determining if that series corresponds to a pre-embedded N-bit identification word. In words, and with reference to Fig. 3, we run through the process steps up through and including the subtracting of the original image from the suspect, but the next step is merely to step through all N random independent signals and perform a simple vector dot product between these signals and the difference signal, and if that dot product is negative, assign a '0' and if that dot product is positive, assign a '1.' Careful analysis of this "one of many" algorithms will show its similarity to the traditional matched filter.

There are also some immediate improvements to the "matched filter" and "correlation-type" that can provide enhanced ability to properly detect very low level embedded code signals. Some of these improvements are derived from principles set forth in the Kassam book, others are generated by the inventor and the inventor has no knowledge of their being developed in other papers or works, but neither has the inventor done fully extensive searching for advanced signal detection techniques. One such technique is perhaps best exemplified by figure 3.5 in Kassam on page 79, wherein there are certain plots of the various locally optimum weighting coefficients which can apply to a general dot-product algorithmic approach to detection. In other words, rather than performing a simple dot product, each elemental multiplication operation in an overall dot product can be weighted based upon known *a priori* statistical

information about the difference signal itself, i.e., the signal within which the low level known signals are being sought. The interested reader who is not already familiar with these topics is encouraged to read chapter 3 of Kassam to gain a fuller understanding.

One principle which did not seem to be explicitly present in the Kassam book and which was developed rudimentarily by the inventor involves the exploitation of the magnitudes of the statistical properties of the known signal being sought relative to the magnitude of the statistical properties of the suspect signal as a whole. In particular, the problematic case seems to be where the embedded signals we are looking for are of much lower level than the noise and corruption present on a difference signal. Fig. 14 attempts to set the stage for the reasoning behind this approach. The top figure 720 contains a generic look at the differences in the histograms between a typical "problematic" difference signal, i.e., a difference signal which has a much higher overall energy than the embedded signals that may or may not be within it. The term "mean-removed" simply means that the means of both the difference signal and the embedded code signal have been removed, a common operation prior to performing a normalized dot product. The lower figure 722 then has a generally similar histogram plot of the derivatives of the two signals, or in the case of an image, the scalar gradients. From pure inspection it can be seen that a simple thresholding operation in the derivative transform domain, with a subsequent conversion back into the signal domain, will go a long way toward removing certain innate biases on the dot product "recognition algorithm" of a few paragraphs back. Thresholding here refers to the idea that if the absolute value of a difference signal derivative value exceeds some threshold, then it is replaced simply by that threshold value. The threshold value can be so chosen to contain most of the histogram of the embedded signal.

Another operation which can be of minor assistance in "alleviating" some of the bias effects in the dot product algorithm is the removal of the low order frequencies in the difference signal, i.e., running the difference signal through a high pass filter, where the cutoff frequency for the high pass filter is relatively near the origin (or DC) frequency.

Special Considerations for Recognizing Embedded Codes on Signals Which Have Been Compressed and Decompressed, or Alternatively, for Recognizing Embedded Codes Within Any Signal Which Has Undergone Some Known Process Which Creates Non-Uniform Error Sources

Long title for a basic concept. Some signal processing operations, such as compressing and decompressing an image, as with the JPEG/MPEG formats of image/video compression, create errors in some given transform domain which have certain correlations and structure. Using JPEG as an example, if a given image is compressed then decompressed at some high compression ratio, and that resulting image is then fourier transformed and compared to the fourier transform of the original uncompressed image, a definite pattern is clearly visible. This patterning is indicative of correlated error, i.e. error which can be to some extent quantified and predicted. The prediction of the grosser properties of this

correlated error can then be used to advantage in the heretofore-discussed methods of recognizing the embedded code signals within some suspect image which may have undergone either JPEG compression or any other operation which leaves these telltale correlated error signatures. The basic idea is that in areas where there are known higher levels of error, the value of the recognition methods is diminished relative to the areas with known lower levels of correlated errors. It is often possible to quantify the expected levels of error and use this quantification to appropriately weight the retransformed signal values. Using JPEG compression again as an example, a suspect signal can be fourier transformed, and the fourier space representation may clearly show the telltale box grid pattern. The fourier space signal can then be "spatially filtered" near the grid points, and this filtered representation can then be transformed back into its regular time or space domain to then be run through the recognition methods presented in this disclosure. Likewise, any signal processing method which creates non-uniform error sources can be transformed into the domain in which these error sources are non-uniform, the values at the high points of the error sources can be attenuated, and the thusly "filtered" signal can be transformed back into the time/space domain for standard recognition. Often this whole process will include the lengthy and arduous step of "characterizing" the typical correlated error behavior in order to "design" the appropriate filtering profiles.

"SIGNATURE CODES" and "INVISIBLE SIGNATURES"

Briefly and for the sake of clarity, the phrases and terms "signatures," "invisible signatures," and "signature codes" have been and will continue to be used to refer to the general techniques of this technology and often refer specifically to the composite embedded code signal as defined early on in this disclosure.

MORE DETAILS ON EMBEDDING SIGNATURE CODES INTO MOTION PICTURES

Just as there is a distinction made between the JPEG standards for compressing still images and the MPEG standards for compressed motion images, so too should there be distinctions made between placing invisible signatures into still images and placing signatures into motion images. As with the JPEG/MPEG distinction, it is not a matter of different foundations, it is the fact that with motion images a new dimension of engineering optimization opens up by the inclusion of time as a parameter. Any textbook dealing with MPEG will surely contain a section on how MPEG is (generally) not merely applying JPEG on a frame by frame basis. It will be the same with the application of the principles of this technology: generally speaking, the placement of invisible signatures into motion image sequences will not be simply independently placing invisible signatures into one frame after the next. A variety of time-based considerations come into play, some dealing with the psychophysics of motion image perception, others driven by simple cost engineering considerations.

One embodiment actually uses the MPEG compression standard as a piece of a solution. Other motion image compression schemes could equally well be used, be they already invented or yet to be invented. This example also utilizes the scrambled logo image approach to generating the master snowy image as depicted in Fig. 13 and discussed in the disclosure.

A "compressed master snowy image" is independently rendered as depicted in Fig. 15. "Rendered" refers to the generally well known technique in video, movie and animation production whereby an image or sequence of images is created by constructive techniques such as computer instructions or the drawing of animation cells by hand. Thus, "to render" a signature movie in this example is essentially to let either a computer create it as a digital file or to design some custom digital electronic circuitry to create it.

The overall goal of the procedure outlined in Fig. 15 is to apply the invisible signatures to the original movie 762 in such a way that the signatures do not degrade the commercial value of the movie, memorialized by the side-by-side viewing, 768, AND in such a way that the signature optimally survives through the MPEG compression and decompression process. As noted earlier, the use of the MPEG process in particular is an example of the generic process of compression. Also it should be noted that the example presented here has definite room for engineering variations. In particular, those practiced in the art of motion picture compression will appreciate the fact if we start out with two video streams A and B, and we compress A and B separately and combine their results, then the resultant video stream C will not generally be the same as if we pre-added the video streams A and B and compressed this resultant. Thus we have in general, e.g.:

$$MPEG(A) + MPEG(B) \;=\backslash=\; MPEG(A+B)$$

where =\= is not equal to. This is somewhat an abstract notion to introduce at this point in the disclosure and will become more clear as Fig. 15 is discussed. The general idea, however, is that there will be a variety of algebras that can be used to optimize the pass-through of "invisible" signatures through compression procedures. Clearly, the same principles as depicted in Fig. 15 also work on still images and the JPEG or any other still image compression standard.

Turning now to the details of Fig. 15, we begin with the simple stepping through of all Z frames of a movie or video. For a two hour movie played at 30 frames per second, Z turns out to be (30*2*60*60) or 216,000. The inner loop of 700, 702 and 704 merely mimics Fig. 13's steps. The logo frame optionally can change during the stepping through frames. The two arrows emanating from the box 704 represent both the continuation of the loop 750 and the depositing of output frames into the rendered master Snowy Image 752.

To take a brief but potentially appropriate digression at this point, the use of the concept of a Markov process brings certain clarity to the discussion of optimizing the engineering implementation of the methods of Fig. 15. Briefly, a Markov process is one in which a sequence of events takes place and in general there is no memory between one step in the sequence and the next. In the context of Fig. 15 and a sequence of images, a Markovian sequence of images would be one in which there is no apparent or appreciable correlation between a given frame and the next. Imagine taking the set of all movies ever produced, stepping one frame at a time and selecting a random frame from a random movie to be inserted into an output movie, and then stepping through, say, one minute or 1800 of these frames. The resulting "movie" would be a fine example of a Markovian movie. One point of this discussion is that depending on how the logo frames are rendered and depending on how the encryption/scrambling step 702 is performed, the Master Snowy Movie 752 will exhibit some generally quantifiable degree of Markovian characteristics. The point of this point is that the compression procedure itself will be affected by this degree of Markovian nature and thus needs to be accounted for in designing the process of Fig. 15. Likewise, and only in general, even if a fully Markovian movie is created in the High Brightness Master Snowy Movie, 752, then the processing of compressing and decompressing that movie 752, represented as the MPEG box 754, will break down some of the Markovian nature of 752 and create at least a marginally non-Markovian compressed master Snowy Movie 756. This point will be utilized when the disclosure briefly discusses the idea of using multiple frames of a video stream in order to find a single N-bit identification word, that is, the same N-bit identification word may be embedded into several frames of a movie, and it is quite reasonable to use the information derived from those multiple frames to find that single N-bit identification word. The non-Markovian nature of 756 thus adds certain tools to reading and recognizing the invisible signatures. Enough of this tangent.

With the intent of pre-conditioning the ultimately utilized Master Snowy Movie 756, we now send the rendered High Brightness Master Snowy Movie 752 through both the MPEG compression AND decompression procedure 754. With the caveat previously discussed where it is acknowledged that the MPEG compression process is generally not distributive, the idea of the step 754 is to crudely segregate the initially rendered Snowy Movie 752 into two components, the component which survives the compression process 754 which is 756, and the component which does not survive, also crudely estimated using the difference operation 758 to produce the "Cheap Master Snowy Movie" 760. The reason use is made of the deliberately loose term "Cheap" is that we can later add this signature signal as well to a distributable movie, knowing that it probably won't survive common compression processes but that nevertheless it can provide "cheap" extra signature signal energy for applications or situations which will never experience compression. [Thus it is at least noted in Fig. 15]. Back to Fig. 15 proper, we now have a rough cut at signatures which we know have a higher likelihood of surviving intact through the compression process, and we use this "Compressed Master Snowy Movie" 756 to then go through this

procedure of being scaled down 764, added to the original movie 766, producing a candidate distributable movie 770, then compared to the original movie (768) to ensure that it meets whatever commercially viable criteria which have been set up (i.e. the acceptable perceived noise level). The arrow from the side-by-side step 768 back to the scale down step 764 corresponds quite directly to the "experiment visually..." step of Fig. 2, and the gain control 226 of Fig. 6. Those practiced in the art of image and audio information theory can recognize that the whole of Fig. 15 can be summarized as attempting to pre-condition the invisible signature signals in such a way that they are better able to withstand even quite appreciable compression. To reiterate a previously mentioned item as well, this idea equally applies to ANY such pre-identifiable process to which an image, and image sequence, or audio track might be subjected. This clearly includes the JPEG process on still images.

Additional Elements of the Realtime Encoder Circuitry

It should be noted that the method steps represented in Fig. 15, generally following from box 750 up through the creation of the compressed master snowy movie 756, could with certain modification be implemented in hardware. In particular, the overall analog noise source 206 in Fig. 6 could be replaced by such a hardware circuit. Likewise the steps and associated procedures depicted in Fig. 13 could be implemented in hardware and replace the analog noise source 206.

Recognition based on more than one frame: non-Markovian signatures

As noted in the digression on Markov and non-Markov sequences of images, it is pointed out once again that in such circumstances where the embedded invisible signature signals are non-Markovian in nature, i.e., that there is some correlation between the master snowy image of one frame to that of the next, AND furthermore that a single N-bit identification word is used across a range of frames and that the sequence of N-bit identification words associated with the sequence of frames is not Markovian in nature, then it is possible to utilize the data from several frames of a movie or video in order to recognize a single N-bit identification word. All of this is a fancy way of saying that the process of recognizing the invisible signatures should use as much information as is available, in this case translating to multiple frames of a motion image sequence.

HEADER VERIFICATION

The concept of the "header" on a digital image or audio file is a well established practice in the art. The top of Fig. 16 has a simplified look at the concept of the header, wherein a data file begins with generally a comprehensive set of information about the file as a whole, often including information about who the author or copyright holder of the data is, if there is a copyright holder at all. This header 800 is

then typically followed by the data itself 802, such as an audio stream, a digital image, a video stream, or compressed versions of any of these items. This is all exceedingly known and common in the industry.

One way in which the principles of this technology can be employed in the service of information integrity is generically depicted in the lower diagram of Fig. 16. In general, the N-bit identification word can be used to essentially "wallpaper" a given simple message throughout an image (as depicted) or audio data stream, thereby reinforcing some message already contained in a traditional header. This is referred to as "header verification" in the title of this section. The thinking here is that less sophisticated would-be pirates and abusers can alter the information content of header information, and the more secure techniques of this technology can thus be used as checks on the veracity of header information. Provided that the code message, such as "joe's image" in the header, matches the repeated message throughout an image, then a user obtaining the image can have some higher degree of confidence that no alteration of the header has taken place.

Likewise, the header can actually carry the N-bit identification word so that the fact that a given data set has been coded via the methods of this technology can be highlighted and the verification code built right into the header. Naturally, this data file format has not been created yet since the principles of this technology are currently not being employed.

THE "BODIER": THE ABILITY TO LARGELY REPLACE A HEADER

Although all of the possible applications of the following aspect of applicant's technology are not fully developed, it is nevertheless presented as a design alternative that may be important some day. The title of this section contains the silly phrase used to describe this possibility: the "bodier."

Whereas the previous section outlined how the N-bit identification word could "verify" information contained within the header of a digital file, there is also the prospect that these methods could completely replace the very concept of the header and place the information which is traditionally stored in the header directly into the digital signal and empirical data itself.

This could be as simple as standardizing on, purely for example, a 96-bit (12 bytes) leader string on an otherwise entirely empirical data stream. This leader string would plain and simple contain the numeric length, in elemental data units, of the entire data file not including the leader string, and the number of bits of depth of a single data element (e.g. its number of grey levels or the number of discrete signal levels of an audio signal). From there, universal codes as described in this specification would be used to read the N-bit identification word written directly within the empirical data. The length of the empirical data would need to be long enough to contain the full N bits. The N-bit word would effectively transmit what would otherwise be contained in a traditional header.

Fig. 17 depicts such a data format and calls it the "universal empirical data format." The leader string 820 is comprised of the 64 bit string length 822 and the 32 bit data word size 824. The data stream

826 then immediately follows, and the information traditionally contained in the header but now contained directly in the data stream is represented as the attached dotted line 828. Another term used for this attached information is a "shadow channel" as also depicted in Fig. 17.

Yet another element that may need to be included in the leader string is some sort of complex check sum bits which can verify that the whole of the data file is intact and unaltered. This is not included in Fig. 17.

MORE ON DISTRIBUTED UNIVERSAL CODE SYSTEMS: DYNAMIC CODES

One intriguing variation on the theme of universal codes is the possibility of the N-bit identification word actually containing instructions which vary the operations of the universal code system itself. One of many examples is immediately in order: a data transmission is begun wherein a given block of audio data is fully transmitted, an N-bit identification word is read knowing that the first block of data used universal codes #145 out of a set of 500, say, and that part of the N-bit identification word thus found is the instructions that the next block of data should be "analyzed" using the universal code set #411 rather than #145. In general, this technology can thus be used as a method for changing on the fly the actual decoding instructions themselves. Also in general, this ability to utilize "dynamic codes" should greatly increase the sophistication level of the data verification procedures and increase the economic viability of systems which are prone to less sophisticated thwarting by hackers and would-be pirates. The inventor does not believe that the concept of dynamically changing decoding/decrypting instructions is novel *per se*, but the carrying of those instructions on the "shadow channel" of empirical data does appear to be novel to the best of the inventor's understanding. [Shadow channel was previously defined as yet another vernacular phrase encapsulating the more steganographic proper elements of this technology].

A variant on the theme of dynamic codes is the use of universal codes on systems which have *a priori* assigned knowledge of which codes to use when. One way to summarize this possibility is the idea of "the daily password." The password in this example represents knowledge of which set of universal codes is currently operative, and these change depending on some set of application-specific circumstances. Presumably many applications would be continually updating the universal codes to ones which had never before been used, which is often the case with the traditional concept of the daily password. Part of a currently transmitted N-bit identification word could be the passing on of the next day's password, for example. Though time might be the most common trigger events for the changing of passwords, there could be event based triggers as well.

SYMMETRIC PATTERNS AND NOISE PATTERNS: TOWARD A ROBUST UNIVERSAL CODING SYSTEM

The placement of identification patterns into images is certainly not new. Logos stamped into corners of images, subtle patterns such as true signatures or the wallpapering of the copyright circle-C symbol, and the watermark proper are all examples of placing patterns into images in order to signify ownership or to try to prevent illicit uses of the creative material.

What does appear to be novel is the approach of placing independent "carrier" patterns, which themselves are capable of being modulated with certain information, directly into images and audio for the purposes of transmission and discernment of said information, while effectively being imperceptible and/or unintelligible to a perceiving human. Steganographic solutions currently known to the inventor all place this information "directly" into empirical data (possibly first encrypted, then directly), whereas the methods of this disclosure posit the creation of these (most-often) coextensive carrier signals, the modulation of those carrier signals with the information proper, THEN the direct application to the empirical data.

In extending these concepts one step further into the application arena of universal code systems, where a sending site transmits empirical data with a certain universal coding scheme employed and a receiving site analyzes said empirical data using the universal coding scheme, it would be advantageous to take a closer look at the engineering considerations of such a system designed for the transmission of images or motion images, as opposed to audio. Said more clearly, the same type of analysis of a specific implementation such as is contained in Fig. 9 and its accompanying discussion on the universal codes in audio applications should as well be done on imagery (or two dimensional signals). This section is such an analysis and outline of a specific implementation of universal codes and it attempts to anticipate various hurdles that such a method should clear.

The unifying theme of one implementation of a universal coding system for imagery and motion imagery is "symmetry." The idea driving this couldn't be more simple: a prophylactic against the use of image rotation as a means for less sophisticated pirates to bypass any given universal coding system. The guiding principle is that the universal coding system should easily be read no matter what rotational orientation the subject imagery is in. These issues are quite common in the fields of optical character recognition and object recognition, and these fields should be consulted for further tools and tricks in furthering the engineering implementation of this technology. As usual, an immediate example is in order.

Digital Video And Internet Company XYZ has developed a delivery system of its product which relies on a non-symmetric universal coding which double checks incoming video to see if the individual frames of video itself, the visual data, contain XYZ's own relatively high security internal signature codes using the methods of this technology. This works well and fine for many delivery situations, including their Internet tollgate which does not pass any material unless both the header information is verified AND the in-frame universal codes are found. However, another piece of their commercial network performs mundane routine monitoring on Internet channels to look for unauthorized transmission of their proprietary creative property. They control the encryption procedures used, thus it is no problem for them to

unencrypt creative property, including headers, and perform straightforward checks. A pirate group that wants to traffic material on XYZ's network has determined how to modify the security features in XYZ's header information system, and they have furthermore discovered that by simply rotating imagery by 10 or 20 degrees, and transmitting it over XYZ's network, the network doesn't recognize the codes and therefore does not flag illicit uses of their material, and the receiver of the pirate's rotated material simply unrotates it.

Summarizing this last example via logical categories, the non-symmetric universal codes are quite acceptable for the "enablement of authorized action based on the finding of the codes," whereas it can be somewhat easily by-passed in the case of "random monitoring (policing) for the presence of codes." [Bear in mind that the non-symmetric universal codes may very well catch 90% of illicit uses, i.e. 90% of the illicit users wouldn't bother even going to the simple by-pass of rotation.] To address this latter category, the use of quasi-rotationally symmetric universal codes is called for. "Quasi" derives from the age old squaring the circle issue, in this instance translating into not quite being able to represent a full incrementally rotational symmetric 2-D object on a square grid of pixels. Furthermore, basic considerations must be made for scale/magnification changes of the universal codes. It is understood that the monitoring process must be performed when the monitored visual material is in the "perceptual" domain, i.e. when it has been unencrypted or unscrambled and in the form with which it is (or would be) presented to a human viewer. Would-be pirates could attempt to use other simple visual scrambling and unscrambling techniques, and tools could be developed to monitor for these telltale scrambled signals. Said another way, would-be pirates would then look to transform visual material out of the perceptual domain, pass by a monitoring point, and then transform the material back into the perceptual domain; tools other than the monitoring for universal codes would need to be used in such scenarios. The monitoring discussed here therefore applies to applications where monitoring can be performed in the perceptual domain, such as when it is actually sent to viewing equipment.

The "ring" is the only full rotationally symmetric two dimensional object. The "disk" can be seen as a simple finite series of concentric and perfectly abutted rings having width along their radial axis. Thus, the "ring" needs to be the starting point from which a more robust universal code standard for images is found. The ring also will fit nicely into the issue of scale/magnification changes, where the radius of a ring is a single parameter to keep track of and account for. Another property of the ring is that even the case where differential scale changes are made to different spatial axes in an image, and the ring turns into an oval, many of the smooth and quasi-symmetric properties that any automated monitoring system will be looking for are generally maintained. Likewise, appreciable geometric distortion of any image will clearly distort rings but they can still maintain gross symmetric properties. Hopefully, more pedestrian methods such as simply "viewing" imagery will be able to detect attempted illicit piracy in these regards, especially when such lengths are taken to by-pass the universal coding system.

Rings to Knots

Having discovered the ring as the only ideal symmetric pattern upon whose foundation a full rotationally robust universal coding system can be built, we must turn this basic pattern into something functional, something which can carry information, can be read by computers and other instrumentation, can survive simple transformations and corruptions, and can give rise to reasonably high levels of security (probably not unbreakable, as the section on universal codes explained) in order to keep the economics of subversion as a simple incremental cost item.

One embodiment of the "ring-based" universal codes is what the inventor refers to as "knot patterns" or simply "knots," in deference to woven Celtic knot patterns which were later refined and exalted in the works of Leonardo Da Vinci (e.g. Mona Lisa, or his knot engravings). Some rumors have it that these drawings of knots were indeed steganographic in nature, i.e. conveying messages and signatures; all the more appropriate. Figs. 18 and 19 explore some of the fundamental properties of these knots.

Two simple examples of knot patterns are depicted by the supra-radial knots, 850 and the radial knots 852. The names of these types are based on the central symmetry point of the splayed rings and whether the constituent rings intersect this point, are fully outside it, or in the case of sub-radial knots the central point would be inside a constituent circle. The examples of 850 and 852 clearly show a symmetrical arrangement of 8 rings or circles. "Rings" is the more appropriate term, as discussed above, in that this term explicitly acknowledges the width of the rings along the radial axis of the ring. It is each of the individual rings in the knot patterns 850 and 852 which will be the carrier signal for a single associated bit plane in our N-bit identification word. Thus, the knot patterns 850 and 852 each are an 8-bit carrier of information. Specifically, assuming now that the knot patterns 850 and 852 are luminous rings on a black background, then the "addition" of a luminous ring to an independent source image could represent a "1" and the "subtraction" of a luminous ring from an independent source image could represent a "0." The application of this simple encoding scheme could then be replicated over and over as in Fig. 19 and its mosaic of knot patterns, with the ultimate step of adding a scaled down version of this encoded (modulated) knot mosaic directly and coextensively to the original image, with the resultant being the distributable image which has been encoded via this universal symmetric coding method. It remains to communicate to a decoding system which ring is the least significant bit in our N-bit identification word and which is the most significant. One such method is to make a slightly ascending scale of radii values (of the individual rings) from the LSB to the MSB. Another is to merely make the MSB, say, 10% larger radius than all the others and to pre-assign counterclockwise as the order with which the remaining bits fall out. Yet another is to put some simple hash mark inside one and only one circle. In other words, there are a variety of ways with which the bit order of the rings can be encoded in these knot patterns.

A procedure for, first, checking for the mere existence of these knot patterns and, second, for reading of the N-bit identification word, is as follows. A suspect image is first fourier transformed via the extremely common 2D FFT computer procedure. Assuming that we don't know the exact scale of the knot patterns, i.e., we don't know the radius of an elemental ring of the knot pattern in the units of pixels, and that we don't know the exact rotational state of a knot pattern, we merely inspect (via basic automated pattern recognition methods) the resulting magnitude of the Fourier transform of the original image for telltale ripple patterns (concentric low amplitude sinusoidal rings on top of the spatial frequency profile of a source image). The periodicity of these rings, along with the spacing of the rings, will inform us that the universal knot patterns are or are not likely present, and their scale in pixels. Classical small signal detection methods can be applied to this problem just as they can to the other detection methodologies of this disclosure. Common spatial filtering can then be applied to the fourier transformed suspect image, where the spatial filter to be used would pass all spatial frequencies which are on the crests of the concentric circles and block all other spatial frequencies. The resulting filtered image would be fourier transformed out of the spatial frequency domain back into the image space domain, and almost by visual inspection the inversion or non-inversion of the luminous rings could be detected, along with identification of the MSB or LSB ring, and the (in this case 8) N-bit identification code word could be found. Clearly, a pattern recognition procedure could perform this decoding step as well.

The preceding discussion and the method it describes has certain practical disadvantages and shortcomings which will now be discussed and improved upon. The basic method was presented in a simple-minded fashion in order to communicate the basic principles involved.

Let's enumerate a few of the practical difficulties of the above described universal coding system using the knot patterns. For one (1), the ring patterns are somewhat inefficient in their "covering" of the full image space and in using all of the information carrying capacity of an image extent. Second (2), the ring patterns themselves will almost need to be more visible to the eye if they are applied, say, in a straightforward additive way to an 8-bit black and white image. Next (3), the "8" rings of Fig. 18, 850 and 852, is a rather low number, and moreover, there is a 22 and one half degree rotation which could be applied to the figures which the recognition methods would need to contend with (360 divided by 8 divided by 2). Next (4), strict overlapping of rings would produce highly condensed areas where the added and subtracted brightness could become quite appreciable. Next (5), the 2D FFT routine used in the decoding is notoriously computationally cumbersome as well as some of the pattern recognition methods alluded to. Finally (6), though this heretofore described form of universal coding does not pretend to have ultra-high security in the classical sense of top security communications systems, it would nevertheless be advantageous to add certain security features which would be inexpensive to implement in hardware and software systems which at the same time would increase the cost of would-be pirates attempting to thwart the system, and increase the necessary sophistication level of those pirates, to the point that a would-be

pirate would have to go so far out of their way to thwart the system that willfulness would be easily proven and hopefully subject to stiff criminal liability and penalty (such as the creation and distribution of tools which strip creative property of these knot pattern codes).

All of these items can be addressed and should continue to be refined upon in any engineering implementation of the principles of the technology. This disclosure addresses these items with reference to the following embodiments.

Beginning with item number 3, that there are only 8 rings represented in Fig. 18 is simply remedied by increasing the number of rings. The number of rings that any given application will utilize is clearly a function of the application. The trade-offs include but are not limited to: on the side which argues to limit the number of rings utilized, there will ultimately be more signal energy per ring (per visibility) if there are less rings; the rings will be less crowded so that there discernment via automated recognition methods will be facilitated; and in general since they are less crowded, the full knot pattern can be contained using a smaller overall pixel extent, e.g. a 30 pixel diameter region of image rather than a 100 pixel diameter region. The arguments to increase the number of rings include: the desire to transmit more information, such as ascii information, serial numbers, access codes, allowed use codes and index numbers, history information, etc.; another key advantage of having more rings is that the rotation of the knot pattern back into itself is reduced, thereby allowing the recognition methods to deal with a smaller range of rotation angles (e.g., 64 rings will have a maximum rotational displacement of just under 3 degrees, i.e. maximally dissimilar to its original pattern, where a rotation of about 5 and one half degrees brings the knot pattern back into its initial alignment; the need to distinguish the MSB/LSB and the bit plane order is better seen in this example as well). It is anticipated that most practical applications will choose between 16 and 128 rings, corresponding to $N=16$ to $N=128$ for the choice of the number of bits in the N-bit identification code word. The range of this choice would somewhat correlate to the overall radius, in pixels, allotted to an elemental knot pattern such as 850 or 852.

Addressing the practical difficulty item number 4, that of the condensation of rings patterns at some points in the image and lack of ring patterns in others (which is very similar, but still distinct from, item 1, the inefficient covering), the following improvement can be applied. Fig. 18 shows an example of a key feature of a "knot" (as opposed to a pattern of rings) in that where patterns would supposedly intersect, a virtual third dimension is posited whereby one strand of the knot takes precedence over another strand in some predefined way; see item 854. In the terms of imagery, the brightness or dimness of a given intersection point in the knot patterns would be "assigned" to one and only one strand, even in areas where more than two strands overlap. The idea here is then extended, 864, to how rules about this assignment should be carried out in some rotationally symmetric manner. For example, a rule would be that, travelling clockwise, an incoming strand to a loop would be "behind" an outgoing strand. Clearly there are a multitude of variations which could be applied to these rules, many which would critically

depend on the geometry of the knot patterns chosen. Other issues involved will probably be that the finite width, and moreover the brightness profile of the width along the normal axis to the direction of a strand, will all play a role in the rules of brightness assignment to any given pixel underlying the knot patterns.

A major improvement to the nominal knot pattern system previously described directly addresses practical difficulties (1), the inefficient covering, (2) the unwanted visibility of the rings, and (6) the need for higher levels of security. This improvement also indirectly address item (4) the overlapping issue, which has been discussed in the last paragraph. This major improvement is the following: just prior to the step where the mosaic of the encoded knot patterns is added to an original image to produce a distributable image, the mosaic of encoded knot patterns, 866, is spatially filtered (using common 2D FFT techniques) by a standardized and (generally smoothly) random phase-only spatial filter. It is very important to note that this phase-only filter is itself fully rotationally symmetric within the spatial frequency domain, i.e. its filtering effects are fully rotationally symmetric. The effect of this phase-only filter on an individual luminous ring is to transform it into a smoothly varying pattern of concentric rings, not totally dissimilar to the pattern on water several instances after a pebble is dropped in, only that the wave patterns are somewhat random in the case of this phase-only filter rather than the uniform periodicity of a pebble wave pattern. Fig. 20 attempts to give a rough (i.e. non-greyscale) depiction of these phase-only filtered ring patterns. The top figure of Fig. 20 is a cross section of a typical brightness contour/profile 874 of one of these phase-only filtered ring patterns. Referenced in the figure is the nominal location of the pre-filtered outer ring center, 870. The center of an individual ring, 872, is referenced as the point around which the brightness profile is rotated in order to fully describe the two dimensional brightness distribution of one of these filtered patterns. Yet another rough attempt to communicate the characteristics of the filtered ring is depicted as 876, a crude greyscale image of the filtered ring. This phase-only filtered ring, 876 will can be referred to as a random ripple pattern.

Not depicted in Fig. 20 is the composite effects of phase-only filtering on the knot patterns of Fig. 18, or on the mosaic of knot patterns 866 in Fig. 19. Each of the individual rings in the knot patterns 850 or 852 will give rise to a 2D brightness pattern of the type 876, and together they form a rather complicated brightness pattern. Realizing that the encoding of the rings is done by making it luminous (1) or "anti-luminous" (0), the resulting phase-only filtered knot patterns begin to take on subtle characteristics which no longer make direct sense to the human eye, but which are still readily discernable to a computer especially after the phase-only filtering is inverse filtered reproducing the original rings patterns.

Returning now to Fig. 19, we can imagine that an 8-bit identification word has been encoded on the knot patterns and the knot patterns phase-only filtered. The resulting brightness distribution would be a rich tapestry of overlapping wave patterns which would have a certain beauty, but would not be readily intelligible to the eye/brain. [An exception to this might draw from the lore of the South Pacific Island communities, where it is said that sea travellers have learned the subtle art of reading small and multiply

complex ocean wave patterns, generated by diffracted and reflected ocean waves off of intervening islands, as a primary navigational tool.] For want of a better term, the resulting mosaic of filtered knot patterns (derived from 866) can be called the encoded knot tapestry or just the knot tapestry. Some basic properties of this knot tapestry are that it retains the basic rotational symmetry of its generator mosaic, it is generally unintelligible to the eye/brain, thus raising it a notch on the sophistication level of reverse engineering, it is more efficient at using the available information content of a grid of pixels (more on this in the next section), and if the basic knot concepts 854 and 864 are utilized, it will not give rise to local "hot spots" where the signal level becomes unduly condensed and hence objectionably visible to a viewer.

The basic decoding process previously described would now need the additional step of inverse filtering the phase-only filter used in the encoding process. This inverse filtering is quite well known in the image processing industry. Provided that the scale of the knot patterns are known *a priori*, the inverse filtering is straightforward. If on the other hand the scale of the knot patterns is not known, then an additional step of discovering this scale is in order. One such method of discovering the scale of the knot patterns is to iteratively apply the inverse phase-only filter to variously scaled version of an image being decoded, searching for which scale-version begins to exhibit noticeable knot patterning. A common search algorithm such as the simplex method could be used in order to accurately discover the scale of the patterns. The field of object recognition should also be consulted, under the general topic of unknown-scale object detection.

An additional point about the efficiency with which the knot tapestry covers the image pixel grid is in order. Most applications of the knot tapestry method of universal image coding will posit the application of the fully encoded tapestry (i.e. the tapestry which has the N-bit identification word embedded) at a relative low brightness level into the source image. In real terms, the brightness scale of the encoded tapestry will vary from, for example, -5 grey scale values to 5 grey scale values in a typical 256 grey scale image, where the preponderance of values will be within -2 and 2. This brings up the purely practical matter that the knot tapestry will be subject to appreciable bit truncation error. Put as an example, imagine a constructed knot tapestry nicely utilizing a full 256 grey level image, then scaling this down by a factor of 20 in brightness including the bit truncation step, then rescaling this truncated version back up in brighmess by the same factor of 20, then inverse phase-only filtering the resultant. The resulting knot pattern mosaic will be a noticeably degraded version of the original knot pattern mosaic. The point of bringing all of this up is the following: it will be a simply defined, but indeed challenging, engineering task to select the various free parameters of design in the implementation of the knot tapestry method, the end goal being to pass a maximum amount of information about the N-bit identification word within some pre-defined visibility tolerance of the knot tapestry. The free parameters include but would not be fully limited to: the radius of the elemental ring in pixels, N or the number of rings, the distance in pixels from the center of a knot pattern to the center of an elemental ring, the packing criteria and

distances of one knot pattern with the others, the rules for strand weaving, and the forms and types of phase-only filters to be used on the knot mosaics. It would be desirable to feed such parameters into a computer optimization routine which could assist in their selection. Even this would begin surely as more of an art than a science due to the many non-linear free parameters involved.

A side note on the use of phase-only filtering is that it can assist in the detection of the ring patterns. It does so in that the inverse filtering of the decoding process tends to "blur" the underlying source image upon which the knot tapestry is added, while at the same time "bringing into focus" the ring patterns. Without the blurring of the source image, the emerging ring patterns would have a harder time "competing" with the sharp features of typical images. The decoding procedure should also utilize the gradient thresholding method described in another section. Briefly, this is the method where if it is known that a source signal is much larger in brightness than our signature signals, then an image being decoded can have higher gradient areas thresholded in the service of increasing the signal level of the signature signals relative to the source signal.

As for the other practical difficulty mentioned earlier, item (5) which deals with the relative computational overhead of the 2D FFT routine and of typical pattern recognition routines, the first remedy here posited but not filled is to find a simpler way of quickly recognizing and decoding the polarity of the ring brightnesses than that of using the 2D FFT. Barring this, it can be seen that if the pixel extent of an individual knot pattern (850 or 852) is, for example, 50 pixels in diameter, than a simple 64 by 64 pixel 2D FFT on some section of an image may be more than sufficient to discern the N-bit identification word as previously described. The idea would be to use the smallest image region necessary, as opposed to being required to utilize an entire image, to discern the N-bit identification word.

Another note is that those practitioners in the science of image processing will recognize that instead of beginning the discussion on the knot tapestry with the utilization of rings, we could have instead jumped right to the use of 2D brightness distribution patterns 876, QUA bases functions. The use of the "ring" terminology as the baseline technology is partly didactic, as is appropriate for patent disclosures in any event. What is more important, perhaps, is that the use of true "rings" in the decoding process, post-inverse filtering, is probably the simplest form to input into typical pattern recognition routines.

Neural Network Decoders

Those skilled in the signal processing art will recognize that computers employing neural network architectures are well suited to the pattern recognition and detection-of-small-signal-in-noise issues posed by the present technology. While a complete discourse on these topics is beyond the scope of this specification, the interested reader is referred to, e.g., Cherkassky, V., "From Statistics to Neural Networks: Theory & Pattern Recognition Applications," Springer-Verlag, 1994; Masters, T., "Signal & Image Processing with Neural Networks: C Sourcebook," Wiley, 1994; Guyon, I, "Advances in Pattern

Recognition Systems Using Neural Networks," World Scientific Publishers, 1994; Nigrin, A., "Neural Networks for Pattern Recognition," MIT Press, 1993; Cichoki, A., "Neural Networks for Optimization & Signal Processing," Wiley, 1993; and Chen, C., "Neural Networks for Pattern Recognition & Their Applications," World Scientific Publishers, 1991.

2D UNIVERSAL CODES II : SIMPLE SCAN LINE IMPLEMENTATION OF THE ONE DIMENSIONAL CASE

The above section on rings, knots and tapestries certainly has its beauty, but some of the steps involved may have enough complexity that practical implementations may be too costly for certain applications. A poor cousin the concept of rings and well-designed symmetry is to simply utilize the basic concepts presented in connection with Fig. 9 and the audio signal, and apply them to two dimensional signals such as images, but to do so in a manner where, for example, each scan line in an image has a random starting point on, for example, a 1000 pixel long universal noise signal. It would then be incumbent upon recognition software and hardware to interrogate imagery across the full range of rotational states and scale factors to "find" the existence of these universal codes.

THE UNIVERSAL COMMERCIAL COPYRIGHT (UCC) IMAGE, AUDIO, AND VIDEO FILE FORMATS

It is as well known as it is regretted that there exist a plethora of file format standards (and not-so-standards) for digital images, digital audio, and digital video. These standards have generally been formed within specific industries and applications, and as the usage and exchange of creative digital material proliferated, the various file formats slugged it out in cross-disciplinary arenas, where today we find a *de facto* histogram of devotees and users of the various favorite formats. The JPEG, MPEG standards for formatting and compression are only slight exceptions it would seem, where some concerted cross-industry collaboration came into play.

The cry for a simple universal standard file format for audio/visual data is as old as the hills. The cry for the protection of such material is older still. With all due respect to the innate difficulties attendant upon the creation of a universal format, and with all due respect to the pretentiousness of outlining such a plan within a patent disclosure, the inventor does believe that these methods can serve perhaps as well as anything for being the foundation upon which an accepted world-wide "universal commercial copyright" format is built. Practitioners know that such animals are not built by proclamation, but through the efficient meeting of broad needs, tenacity, and luck. More germane to the purposes of this disclosure is the fact that the application of this technology would benefit if it could become a central piece within an industry standard file format. The use of universal codes in particular could be specified within such a

standard. The fullest expression of the commercial usage of this technology comes from the knowledge that the invisible signing is taking place and the confidence that instills in copyright holders.

The following is a list of reasons that the principles of this technology could serve as the catalyst for such a standard: (1) Few if any technical developments have so isolated and so pointedly addressed the issue of broad-brush protection of empirical data and audio/visual material; (2) All previous file formats have treated the information about the data, and the data itself, as two separate and physically distinct entities, whereas the methods of this technology can combine the two into one physical entity; (3) The mass scale application of the principles of this technology will require substantial standardization work in the first place, including integration with the years-to-come improvements in compression technologies, so the standards infrastructure will exist by default; (4) the growth of multimedia has created a generic class of data called "content," which includes text, images, sound, and graphics, arguing for higher and higher levels of "content standards"; and (5) marrying copyright protection technology and security features directly into a file format standard is long overdue.

Elements of a universal standard would certainly include the mirroring aspects of the header verification methods, where header information is verified by signature codes directly within data. Also, a universal standard would outline how hybrid uses of fully private codes and public codes would commingle. Thus, if the public codes were "stripped" by sophisticated pirates, the private codes would remain intact. A universal standard would specify how invisible signatures would evolve as digital images and audio evolve. Thus, when a given image is created based on several source images, the standard would specify how and when the old signatures would be removed and replaced by new signatures, and if the header would keep track of these evolutions and if the signatures themselves would keep some kind of record.

PIXELS VS. BUMPS

Most of the disclosure focuses on pixels being the basic carriers of the N-bit identification word. The section discussing the use of a single "master code signal" went so far as to essentially "assign" each and every pixel to a unique bit plane in the N-bit identification word.

For many applications, with one exemplar being that of ink based printing at 300 dots per inch resolution, what was once a pixel in a pristine digital image file becomes effectively a blob (e.g. of dithered ink on a piece of paper). Often the isolated information carrying capacity of the original pixel becomes compromised by neighboring pixels spilling over into the geometrically defined space of the original pixel. Those practiced in the art will recognize this as simple spatial filtering and various forms of blurring.

In such circumstances it may be more advantageous to assign a certain highly local group of pixels to a unique bit plane in the N-bit identification word, rather than merely a single pixel. The end goal is

simply to pre-concentrate more of the signature signal energy into the lower frequencies, realizing that most practical implementations quickly strip or mitigate higher frequencies.

A simple-minded approach would be to assign a 2 by 2 block of pixels all to be modulated with the same ultimate signature grey value, rather than modulating a single assigned pixel. A more fancy approach is depicted in Figs. 21A and 21B, where an array of pixel groups is depicted. This is a specific example of a large class of configurations. The idea is that now a certain small region of pixels is associated with a given unique bit plane in the N-bit identification word, and that this grouping actually shares pixels between bit planes (though it doesn't necessary have to share pixels, as in the case of a 2x2 block of pixels above).

Depicted in Figs. 21A and 21B is a 3x3 array of pixels with an example normalized weighting (normalized --> the weights add up to 1). The methods of this technology now operate on this elementary "bump," as a unit, rather than on a single pixel. It can be seen that in this example there is a fourfold decrease in the number of master code values that need to be stored, due to the spreading out of the signature signal. Applications of this "bump approach" to placing in invisible signatures include any application which will experience *a priori* known high amounts of blurring, where proper identification is still desired even after this heavy blurring.

MORE ON THE STEGANOGRAPHIC USES OF THIS TECHNOLOGY

As mentioned in the initial sections of the disclosure, steganography as an art and as a science is a generic prior art to this technology. Putting the shoe on the other foot now, and as already doubtless apparent to the reader who has ventured thus far, the methods of this technology can be used as a novel method for performing steganography. (Indeed, all of the discussion thus far may be regarded as exploring various forms and implementations of steganography.)

In the present section, we shall consider steganography as the need to pass a message from point A to point B, where that message is essentially hidden within generally independent empirical data. As anyone in the industry of telecommunications can attest to, the range of purposes for passing messages is quite broad. Presumably there would be some extra need, beyond pure hobby, to place messages into empirical data and empirical signals, rather than sending those messages via any number of conventional and straightforward channels. Past literature and product propaganda within steganography posits that such an extra need, among others, might be the desire to hide the fact that a message is even being sent. Another possible need is that a conventional communications channel is not available directly or is cost prohibitive, assuming, that is, that a sender of messages can "transmit" their encoded empirical data somehow. This disclosure includes by reference all previous discussions on the myriad uses to which steganography might apply, while adding the following uses which the inventor has not previously seen described.

The first such use is very simple. It is the need to carry messages about the empirical data within which the message is carried. The little joke is that now the media is truly the message, though it would be next to impossible that some previous steganographer hasn't already exploited this joke. Some of the discussion on placing information about the empirical data directly inside that empirical data was already covered in the section on replacing the header and the concept of the "bodier." This section expands upon that section somewhat.

The advantages of placing a message about empirical data directly in that data is that now only one class of data object is present rather than the previous two classes. In any two class system, there is the risk of the two classes becoming disassociated, or one class corrupted without the other knowing about it. A concrete example here is what the inventor refers to as "device independent instructions."

There exist zillions of machine data formats and data file formats. This plethora of formats has been notorious in its power to impede progress toward universal data exchange and having one machine do the same thing that another machine can do. The instructions that an originator might put into a second class of data (say the header) may not at all be compatible with a machine which is intended to recognize these instructions. If format conversions have taken place, it is also possible that critical instructions have been stripped along the way, or garbled. The improvements disclosed here can be used as a way to "seal in" certain instructions directly into empirical data in such a way that all that is needed by a reading machine to recognize instructions and messages is to perform a standardized "recognition algorithm" on the empirical data (providing of course that the machine can at the very least "read" the empirical data properly). All machines could implement this algorithm any old way they choose, using any compilers or internal data formats that they want.

Implementation of this device independent instruction method would generally not be concerned over the issue of piracy or illicit removal of the sealed in messages. Presumably, the embedded messages and instructions would be a central valuable component in the basic value and functioning of the material.

Another example of a kind of steganographic use of the technology is the embedding of universal use codes for the benefit of a user community. The "message" being passed could be simply a registered serial number identifying ownership to users who wish to legitimately use and pay for the empirical information. The serial number could index into a vast registry of creative property, containing the name or names of the owners, pricing information, billing information, and the like. The "message" could also be the clearance of free and public use for some given material. Similar ownership identification and use indexing can be achieved in two class data structure methods such as a header, but the use of the single class system of this technology may offer certain advantages over the two class system in that the single class system does not care about file format conversion, header compatibilities, internal data format issues, header/body archiving issues, and media transformations.

Fully Exact Steganography

Prior art steganographic methods currently known to the inventor generally involve fully deterministic or "exact" prescriptions for passing a message. Another way to say this is that it is a basic assumption that for a given message to be passed correctly in its entirety, the receiver of the information needs to receive the exact digital data file sent by the sender, tolerating no bit errors or "loss" of data. By definition, "lossy" compression and decompression on empirical signals defeat such steganographic methods. (Prior art, such as the previously noted Komatsu work, are the exceptions here.)

The principles of this technology can also be utilized as an exact form of steganography proper. It is suggested that such exact forms of steganography, whether those of prior art or those of this technology, be combined with the relatively recent art of the "digital signature" and/or the DSS (digital signature standard) in such a way that a receiver of a given empirical data file can first verify that not one single bit of information has been altered in the received file, and thus verify that the contained exact steganographic message has not been altered.

The simplest way to use the principles of this technology in an exact steganographic system is to utilize the previously discussed "designed" master noise scheme wherein the master snowy code is not allowed to contain zeros. Both a sender and a receiver of information would need access to BOTH the master snowy code signal AND the original unencoded original signal. The receiver of the encoded signal merely subtracts the original signal giving the difference signal and the techniques of simple polarity checking between the difference signal and the master snowy code signal, data sample to data sample, producing a the passed message a single bit at a time. Presumably data samples with values near the "rails" of the grey value range would be skipped (such as the values 0,1,254 and 255 in 8-bit depth empirical data).

Statistical Steganography

The need for the receiver of a steganographic embedded data file to have access to the original signal can be removed by turning to what the inventor refers to as "statistical steganography." In this approach, the methods of this technology are applied as simple *a priori* rules governing the reading of an empirical data set searching for an embedded message. This method also could make good use of it combination with prior art methods of verifying the integrity of a data file, such as with the DSS. (See, e.g., Walton, "Image Authentication for a Slippery New Age," Dr. Dobb's Journal, April, 1995, p. 18 for methods of verifying the sample-by-sample, bit-by-bit, integrity of a digital image.)

Statistical steganography posits that a sender and receiver both have access to the same master snowy code signal. This signal can be entirely random and securely transmitted to both parties, or generated by a shared and securely transmitted lower order key which generates a larger quasi-random master snowy code signal. It is *a priori* defined that 16 bit chunks of a message will be passed within

contiguous 1024 sample blocks of empirical data, and that the receiver will use dot product decoding methods as outlined in this disclosure. The sender of the information pre-checks that the dot product approach indeed produces the accurate 16 bit values (that is, the sender pre-checks that the cross-talk between the carrier image and the message signal is not such that the dot product operation will produce an unwanted inversion of any of the 16 bits). Some fixed number of 1024 sample blocks are transmitted and the same number times 16 bits of message is therefore transmitted. DSS techniques can be used to verify the integrity of a message when the transmitted data is known to only exist in digital form, whereas internal checksum and error correcting codes can be transmitted in situations where the data may be subject to change and transformation in its transmission. In this latter case, it is best to have longer blocks of samples for any given message content size (such as 10K samples for a 16 bit message chunk, purely as an example).

Continuing for a moment on the topic of error correcting steganography, it will be recognized that many decoding techniques disclosed herein operate on the principle of distinguishing pixels (or bumps) which have been augmented by the encoded data from those that have been diminished by the encoded data. The distinguishing of these positive and negative cases becomes increasingly difficult as the delta values (e.g. the difference between an encoded pixel and the corresponding original pixel) approach zero.

An analogous situation arises in certain modem transmission techniques, wherein an ambiguous middle ground separates the two desired signal states (e.g. +/- 1). Errors deriving from incorrect interpretation of this middle ground are sometimes termed "soft errors." Principles from modem technology, and other technologies where such problems arise, can likewise be applied to mitigation of such errors in the present context.

One approach is to weight the "confidence" of each delta determination. If the pixel (bump) clearly reflects one state or the other (e.g. +/- 1), its "confidence" is said to be high, and it is given a proportionately greater weighting. Conversely, if the pixel (bump) is relatively ambiguous in its interpretation, its confidence is commensurately lower, and it is given a proportionately lesser weighting. By weighting the data from each pixel (bump) in accordance with its confidence value, the effects of soft errors can be greatly reduced.

The foregoing procedure, while theoretically simple, relies on weightings which are best determined empirically. Accordingly, such an approach is not necessarily straightforward.

An alternative approach is to assign confidence values not to interpretations of individual pixels, but rather to determination of bit values -- either from an image excerpt, or across the entire image. In such an arrangement, each decoded message bit is given a confidence value depending on the ambiguity (or not) of the image statistics by which its value was determined.

Such confidence weighting can also be used as a helpful adjunct with other error detecting/correcting schemes. For example, in known error correcting polynomials, the above-detailed weighting parameters can be used to further hone polynomial-based discernment of an error's location.

THE "NOISE" IN VECTOR GRAPHICS AND VERY-LOW-ORDER INDEXED GRAPHICS

The methods of this disclosure generally posit the existence of "empirical signals," which is another way of saying signals which have noise contained within them almost by definition. There are two classes of 2 dimensional graphics which are not generally considered to have noise inherent in them: vector graphics and certain indexed bit-mapped graphics. Vector graphics and vector graphic files are generally files which contain exact instructions for how a computer or printer draws lines, curves and shapes. A change of even one bit value in such a file might change a circle to a square, as a very crude example. In other words, there is generally no "inherent noise" to exploit within these files. Indexed bit-mapped graphics refers to images which are composed of generally a small number of colors or grey values, such as 16 in the early CGA displays on PC computers. Such "very-low-order" bit-mapped images usually display graphics and cartoons, rather than being used in the attempted display of a digital image taken with a camera of the natural world. These types of very-low-order bit-mapped graphics also are generally not considered to contain "noise" in the classic sense of that term. The exception is where indexed graphic files do indeed attempt to depict natural imagery, such as with the GIF (graphic interchange format of Compuserve), where the concept of "noise" is still quite valid and the principles of this technology still quite valid. These latter forms often use dithering (similar to pointillist paintings and color newspaper print) to achieve near lifelike imagery.

This section concerns this class of 2 dimensional graphics which traditionally do not contain "noise." This section takes a brief look at how the principles of this technology can still be applied in some fashion to such creative material.

The easiest way to apply the principles of this technology to these "noiseless" graphics is to convert them into a form which is amenable to the application of the principles of this technology. Many terms have been used in the industry for this conversion, including "ripping" a vector graphic (raster image processing) such that a vector graphic file is converted to a greyscale pixel-based raster image. Programs such as Photoshop by Adobe have such internal tools to convert vector graphic files into RGB or greyscale digital images. Once these files are in such a form, the principles of this technology can be applied in a straightforward manner. Likewise, very-low-indexed bitmaps can be converted to an RGB digital image or an equivalent. In the RGB domain, the signatures can be applied to the three color channels in appropriate ratios, or the RGB image can be simply converted into a greyscale/chroma format such as "Lab" in Adobe's Photoshop software, and the signatures can be applied to the "Lightness channel" therein. Since most of the distribution media, such as videotapes, CD-ROMs, MPEG video, digital images, and print are

all in forms which are amenable to the application of the principles of this technology, this conversion from vector graphic form and very-low-order graphic form is often done in any event.

Another way to apply the principles of this technology to vector graphics and very-low-order bitmapped graphics is to recognize that, indeed, there are certain properties to these inherent graphic formats which - to the eye - appear as noise. The primary example is the borders and contours between where a given line or figure is drawn or not drawn, or exactly where a bit-map changes from green to blue. In most cases, a human viewer of such graphics will be keenly aware of any attempts to "modulate signature signals" via the detailed and methodical changing of the precise contours of a graphic object. Nevertheless, such encoding of the signatures is indeed possible. The distinction between this approach and that disclosed in the bulk of this disclosure is that now the signatures must ultimately derive from what already exists in a given graphic, rather than being purely and separately created and added into a signal. This disclosure points out the possibilities here nonetheless. The basic idea is to modulate a contour, a touch right or a touch left, a touch up or a touch down, in such a way as to communicate an N-bit identification word. The locations of the changes contours would be contained in a an analogous master noise image, though now the noise would be a record of random spatial shifts one direction or another, perpendicular to a given contour. Bit values of the N-bit identification word would be encoded, and read, using the same polarity checking method between the applied change and the change recorded in the master noise image.

PLASTIC CREDIT AND DEBIT CARD SYSTEMS BASED ON THE PRINCIPLES OF THE TECHNOLOGY

Growth in the use of plastic credit cards, and more recently debit cards and ATM cash cards, needs little introduction. Nor does there need to be much discussion here about the long history of fraud and illicit uses of these financial instruments. The development of the credit card hologram, and its subsequent forgery development, nicely serves as a historic example of the give and take of plastic card security measures and fraudulent countermeasures. This section will concern itself with how the principles of this technology can be realized in an alternative, highly fraud-proof yet cost effective plastic card-based financial network.

A basic list of desired features for an ubiquitous plastic economy might be as follows: 1) A given plastic financial card is completely impossible to forge; 2) An attempted forged card (a "look-alike") cannot even function within a transaction setting; 3) Intercepted electronic transactions by a would-be thief would not in any way be useful or re-useable; 4) In the event of physical theft of an actual valid card, there are still formidable obstacles to a thief using that card; and 5) The overall economic cost of implementation of the financial card network is equal to or less than that of the current international credit card networks, i.e., the fully loaded cost per transaction is equal to or less than the current norm, allowing

for higher profit margins to the implementors of the networks. Apart from item 5, which would require a detailed analysis of the engineering and social issues involved with an all out implementation strategy, the following use of the principles of this technology may well achieve the above list, even item 5.

Figs. 22 through 26, along with the ensuing written material, collectively outline what is referred to in Fig. 26 as "The Negligible-Fraud Cash Card System." The reason that the fraud-prevention aspects of the system are highlighted in the title is that fraud, and the concomitant lost revenue therefrom, is apparently a central problem in today's plastic card based economies. The differential advantages and disadvantages of this system relative to current systems will be discussed after an illustrative embodiment is presented.

Fig. 22 illustrates the basic unforgeable plastic card which is quite unique to each and every user. A digital image 940 is taken of the user of the card. A computer, which is hooked into the central accounting network, 980, depicted in Fig. 26, receives the digital image 940, and after processing it (as will be described surrounding Fig. 24) produces a final rendered image which is then printed out onto the personal cash card 950. Also depicted in Fig. 22 is a straightforward identification marking, in this case a bar code 952, and optional position fiducials which may assist in simplifying the scanning tolerances on the Reader 958 depicted in Fig. 23.

The short story is that the personal cash card 950 actually contains a very large amount of information unique to that particular card. There are no magnetic strips involved, though the same principles can certainly be applied to magnetic strips, such as an implanted magnetic noise signal (see earlier discussion on the "fingerprinting" of magnetic strips in credit cards; here, the fingerprinting would be prominent and proactive as opposed to passive). In any event, the unique information within the image on the personal cash card 950 is stored along with the basic account information in a central accounting network, 980, Fig. 26. The basis for unbreakable security is that during transactions, the central network need only query a small fraction of the total information contained on the card, and never needs to query the same precise information on any two transactions. Hundreds if not thousands or even tens of thousands of unique and secure "transaction tokens" are contained within a single personal cash card. Would-be pirates who went so far as to pick off transmissions of either encrypted or even unencrypted transactions would find the information useless thereafter. This is in marked distinction to systems which have a single complex and complete "key" (generally encrypted) which needs to be accessed, in its entirety, over and over again. The personal cash card on the other hand contains thousands of separate and secure keys which can be used once, within milliseconds of time, then forever thrown away (as it were). The central network 980 keeps track of the keys and knows which have been used and which haven't.

Fig. 23 depicts what a typical point-of-sale reading device, 958, might look like. Clearly, such a device would need to be manufacturable at costs well in line with, or cheaper than, current cash register

systems, ATM systems, and credit card swipers. Not depicted in Fig. 23 are the innards of the optical scanning, image processing, and data communications components, which would simply follow normal engineering design methods carrying out the functions that are to be described henceforth and are well within the capability of artisans in these fields. The reader 958 has a numeric punch pad 962 on it, showing that a normal personal identification number system can be combined with the overall design of this system adding one more conventional layer of security (generally after a theft of the physical card has occurred). It should also be pointed out that the use of the picture of the user is another strong (and increasingly common) security feature intended to thwart after-theft and illicit use. Functional elements such as the optical window, 960, are shown, mimicking the shape of the card, doubling as a centering mechanism for the scanning. Also shown is the data line cable 966 presumably connected either to a proprietor's central merchant computer system or possibly directly to the central network 980. Such a reader may also be attached directly to a cash register which performs the usual tallying of purchased items. Perhaps overkill on security would be the construction of the reader, 958, as a type of Faraday cage such that no electronic signals, such as the raw scan of the card, can emanate from the unit. The reader 958 does need to contain, preferably, digital signal processing units which will assist in swiftly calculating the dot product operations described henceforth. It also should contain local read-only memory which stores a multitude of spatial patterns (the orthogonal patterns) which will be utilized in the "recognition" steps outlined in Fig. 25 and its discussion. As related in Fig. 23, a consumer using the plastic card merely places their card on the window to pay for a transaction. A user could choose for themselves if they want to use a PIN number or not. Approval of the purchase would presumably happen within seconds, provided that the signal processing steps of Fig. 25 are properly implemented with effectively parallel digital processing hardware.

Fig. 24 takes a brief look at one way to process the raw digital image, 940, of a user into an image with more useful information content and uniqueness. It should be clearly pointed out that the raw digital image itself could in fact be used in the following methods, but that placing in additional orthogonal patterns into the image can significantly increase the overall system. (Orthogonal means that, if a given pattern is multiplied by another orthogonal pattern, the resulting number is zero, where "multiplication of patterns" is meant in the sense of vector dot products; these are all familiar terms and concepts in the art of digital image processing). Fig. 24 shows that the computer 942 can, after interrogating the raw image 970, generate a master snowy image 972 which can be added to the raw image 970 to produce a yet-more unique image which is the image that is printed onto the actual personal cash card, 950. The overall effect on the image is to "texturize" the image. In the case of a cash card, invisibility of the master snowy pattern is not as much of a requirement as with commercial imagery, and one of the only criteria for keeping the master snowy image somewhat lighter is to not obscure the image of the user. The central network, 980, stores the final processed image in the record of the account of the user, and it is this

unique and securely kept image which is the carrier of the highly secure "throw-away transaction keys." This image will therefore be "made available" to all duly connected point-of-sale locations in the overall network. As will be seen, none of the point-of-sale locations ever has knowledge of this image, they merely answer queries from the central network.

Fig. 25 steps through a typical transaction sequence. The figure is laid out via indentations, where the first column are steps performed by the point-of-sale reading device 958, the second column has information transmission steps communicated over the data line 966, and the third column has steps taken by the central network 980 which has the secured information about the user's account and the user's unique personal cash card 950. Though there is some parallelism possible in the implementation of the steps, as is normally practiced in the engineering implementation of such systems, the steps are nevertheless laid out according to a general linear sequence of events.

Step one of Fig. 25 is the standard "scanning" of a personal cash card 950 within the optical window 960. This can be performed using linear optical sensors which scan the window, or via a two dimensional optical detector array such as a CCD. The resulting scan is digitized into a grey scale image and stored in an image frame memory buffer such as a "framegrabber," as is now common in the designs of optical imaging systems. Once the card is scanned, a first image processing step would probably be locating the four fiducial center points, 954, and using these four points to guide all further image processing operations (i.e. the four fiducials "register" the corresponding patterns and barcodes on the personal cash card). Next, the barcode ID number would be extracted using common barcode reading image processing methods. Generally, the user's account number would be determined in this step.

Step two of Fig. 25 is the optional typing in of the PIN number. Presumably most users would opt to have this feature, except those users who have a hard time remembering such things and who are convinced that no one will ever steal their cash card.

Step three of Fig. 25 entails connecting through a data line to the central accounting network and doing the usual communications handshaking as is common in modem-based communications systems. A more sophisticated embodiment of this system would obviate the need for standard phone lines, such as the use of optical fiber data links, but for now we can assume it is a garden variety belltone phone line and that the reader 958 hasn't forgotten the phone number of the central network.

After basic communications are established, step four shows that the point-of-sale location transmits the ID number found in step 1, along with probably an encrypted version of the PIN number (for added security, such as using the ever more ubiquitous RSA encryption methods), and appends the basic information on the merchant who operates the point-of-sale reader 958, and the amount of the requested transaction in monetary units.

Step five has the central network reading the ID number, routing the information accordingly to the actual memory location of that user's account, thereafter verifying the PIN number and checking that

the account balance is sufficient to cover the transaction. Along the way, the central network also accesses the merchant's account, checks that it is valid, and readies it for an anticipated credit.

Step six begins with the assumption that step five passed all counts. If step five didn't, the exit step of sending a NOT OK back to the merchant is not depicted. So, if everything checks out, the central network generates twenty four sets of sixteen numbers, where all numbers are mutually exclusive, and in general, there will be a large but quite definitely finite range of numbers to choose from. Fig. 25 posits the range being 64K or 65536 numbers. It can be any practical number, actually. Thus, set one of the twenty four sets might have the numbers 23199, 54142, 11007, 2854, 61932, 32879, 38128, 48107, 65192, 522, 55723, 27833, 19284, 39970, 19307, and 41090, for example. The next set would be similarly random, but the numbers of set one would be off limits now, and so on through the twenty four sets. Thus, the central network would send (16x24x2 bytes) of numbers or 768 bytes. The actual amount of numbers can be determined by engineering optimization of security versus transmission speed issues. These random numbers are actually indexes to a set of 64K universally *a priori* defined orthogonal patterns which are well known to both the central network and are permanently stored in memory in all of the point-of-sale readers. As will be seen, a would-be thief's knowledge of these patterns is of no use.

Step seven then transmits the basic "OK to proceed" message to the reader, 958, and also sends the 24 sets of 16 random index numbers.

Step eight has the reader receiving and storing all these numbers. Then the reader, using its local microprocessor and custom designed high speed digital signal processing circuitry, steps through all twenty four sets of numbers with the intention of deriving 24 distinct floating point numbers which it will send back to the central network as a "one time key" against which the central network will check the veracity of the card's image. The reader does this by first adding together the sixteen patterns indexed by the sixteen random numbers of a given set, and then performing a common dot product operation between the resulting composite pattern and the scanned image of the card. The dot product generates a single number (which for simplicity we can call a floating point number). The reader steps through all twenty four sets in like fashion, generating a unique string of twenty four floating point numbers.

Step nine then has the reader transmitting these results back to the central network.

Step ten then has the central network performing a check on these returned twenty four numbers, presumably doing its own exact same calculations on the stored image of the card that the central network has in its own memory. The numbers sent by the reader can be "normalized," meaning that the highest absolute value of the collective twenty four dot products can divided by itself (its unsigned value), so that brightness scale issues are removed. The resulting match between the returned values and the central network's calculated values will either be well within given tolerances if the card is valid, and way off if the card is a phony or if the card is a crude reproduction.

Step eleven then has the central network sending word whether or not the transaction was OK, and letting the customer know that they can go home with their purchased goods.

Step twelve then explicitly shows how the merchant's account is credited with the transaction amount.

As already stated, the primary advantage of this plastic card is to significantly reduce fraud, which apparently is a large cost to current systems. This system reduces the possibility of fraud only to those cases where the physical card is either stolen or very carefully copied. In both of these cases, there still remains the PIN security and the user picture security (a known higher security than low wage clerks analyzing signatures). Attempts to copy the card must be performed through "temporary theft" of the card, and require photo-quality copying devices, not simple magnetic card swipers. The system is founded upon a modern 24 hour highly linked data network. Illicit monitoring of transactions does the monitoring party no use whether the transmissions are encrypted or not.

It will be appreciated that the foregoing approach to increasing the security of transactions involving credit and debit card systems is readily extended to any photograph-based identification system. Moreover, the principles of the present technology may be applied to detect alteration of photo ID documents, and to generally enhance the confidence and security of such systems. In this regard, reference is made to Fig. 28, which depicts a photo-ID card or document 1000 which may be, for example, a passport, visa, permanent resident card ("green card"), driver's license, credit card, government employee identification, or a private industry identification badge. For convenience, such photograph-based identification documents will be collectively referred to as photo ID documents.

The photo ID document includes a photograph 1010 that is attached to the document 1000. Printed, human-readable information 1012 is incorporated in the document 1000, adjacent to the photograph 1010. Machine readable information, such as that known as "bar code" may also be included adjacent to the photograph.

Generally, the photo ID document is constructed so that tampering with the document (for example, swapping the original photograph with another) should cause noticeable damage to the card. Nevertheless, skilled forgerers are able to either alter existing documents or manufacture fraudulent photo ID documents in a manner that is extremely difficult to detect.

As noted above, the present technology enhances the security associated with the use of photo ID documents by supplementing the photographic image with encoded information (which information may or may not be visually perceptible), thereby facilitating the correlation of the photographic image with other information concerning the person, such as the printed information 1012 appearing on the document 1000.

In one embodiment, the photograph 1010 may be produced from a raw digital image to which is added a master snowy image as described above in connection with Figs. 22-24. The above-described

central network and point-of-sale reading device (which device, in the present embodiment, may be considered as a point-of-entry or point-of-security photo ID reading device), would essentially carry out the same processing as described with that embodiment, including the central network generation of unique numbers to serve as indices to a set of defined orthogonal patterns, the associated dot product operation carried out by the reader, and the comparison with a similar operation carried out by the central network. If the numbers generated from the dot product operation carried out by the reader and the central network match, in this embodiment, the network sends the OK to the reader, indicating a legitimate or unaltered photo ID document.

In another embodiment, the photograph component 1010 of the identification document 1000 may be digitized and processed so that the photographic image that is incorporated into the photo ID document 1000 corresponds to the "distributable signal" as defined above. In this instance, therefore, the photograph includes a composite, embedded code signal, imperceptible to a viewer, but carrying an N-bit identification code. It will be appreciated that the identification code can be extracted from the photo using any of the decoding techniques described above, and employing either universal or custom codes, depending upon the level of security sought.

It will be appreciated that the information encoded into the photograph may correlate to, or be redundant with, the readable information 1012 appearing on the document. Accordingly, such a document could be authenticated by placing the photo ID document on a scanning system, such as would be available at a passport or visa control point. The local computer, which may be provided with the universal code for extracting the identification information, displays the extracted information on the local computer screen so that the operator is able to confirm the correlation between the encoded information and the readable information 1012 carried on the document.

It will be appreciated that the information encoded with the photograph need not necessarily correlate with other information on an identification document. For example, the scanning system may need only to confirm the existence of the identification code so that the user may be provided with a "go" or "no go" indication of whether the photograph has been tampered with. It will also be appreciated that the local computer, using an encrypted digital communications line, could send a packet of information to a central verification facility, which thereafter returns an encrypted "go" or "no go" indication.

In another embodiment, it is contemplated that the identification code embedded in the photograph may be a robust digital image of biometric data, such as a fingerprint of the card bearer, which image, after scanning and display, may be employed for comparison with the actual fingerprint of the bearer in very high security access points where on-the-spot fingerprint recognition systems (or retinal scans, etc.) are employed.

It will be appreciated that the information embedded in the photograph need not be visually hidden or steganographically embedded. For example, the photograph incorporated into the identification card

may be a composite of an image of the individual and one-, or two-dimensional bar codes. The bar code information would be subject to conventional optical scanning techniques (including internal cross checks) so that the information derived from the code may be compared, for example, to the information printed on the identification document.

It is also contemplated that the photographs of ID documents currently in use may be processed so that information correlated to the individual whose image appears in the photograph may be embedded. In this regard, the reader's attention is directed to the foregoing portion of this description entitled "Use in Printing, Paper, Documents, Plastic-Coated Identification Cards, and Other Material Where Global Embedded Codes Can Be Imprinted," wherein there is described numerous approaches to modulation of physical media that may be treated as "signals" amenable to application of the present technology principles.

NETWORK LINKING METHOD USING INFORMATION EMBEDDED IN DATA OBJECTS THAT HAVE INHERENT NOISE

The diagram of Fig. 27 illustrates the aspect of the technology that provides a network linking method using information embedded in data objects that have inherent noise. In one sense, this aspect is a network navigation system and, more broadly, a massively distributed indexing system that embeds addresses and indices directly within data objects themselves. As noted, this aspect is particularly well-adapted for establishing hot links with pages presented on the World Wide Web (WWW). A given data object effectively contains both a graphical representation and embedded URL address.

As in previous embodiments, this embedding is carried out so that the added address information does not affect the core value of the object so far as the creator and audience are concerned. As a consequence of such embedding, only one class of data objects is present rather than the two classes (data object and discrete header file) that are attendant with traditional WWW links. The advantages of reducing a hot-linked data object to a single class were mentioned above, and are elaborated upon below. In one embodiment of the technology, the World Wide Web is used as a pre-existing hot link based network. The common apparatus of this system is networked computers and computer monitors displaying the results of interactions when connected to the web. This embodiment of the technology contemplates steganographically embedding URL or other address-type information directly into images, videos, audio, and other forms of data objects that are presented to a web site visitor, and which have "gray scale" or "continuous tones" or "gradations" and, consequently, inherent noise. As noted above, there are a variety of ways to realize basic steganographic implementations, all of which could be employed in accordance with the present technology.

With particular reference to Fig. 27, images, quasi-continuous tone graphics, multimedia video and audio data are currently the basic building blocks of many sites 1002, 1004 on the World Wide Web.

Such data will be hereafter collectively referred to as creative data files or data objects. For illustrative purposes, a continuous-tone graphic data object 1006 (diamond ring with background) is depicted in Fig. 27.

Web site tools - both those that develop web sites 1008 and those that allow browsing them 1010 - routinely deal with the various file formats in which these data objects are packaged. It is already common to distribute and disseminate these data objects 1006 as widely as possible, often with the hope on a creator's part to sell the products represented by the objects or to advertise creative services (e.g., an exemplary photograph, with an 800 phone number displayed within it, promoting a photographer's skills and service). Using the methods of this technology, individuals and organizations who create and disseminate such data objects can embed an address link that leads right back to their own node on a network, their own site on the WWW.

A user at one site 1004 needs merely to point and click at the displayed object 1006. The software 1010 identifies the object as a hot link object. The software reads the URL address that is embedded within the object and routes the user to the linked web site 1002, just as if the user had used a conventional web link. That linked site 1002 is the home page or network node of the creator of the object 1006, which creator may be a manufacturer. The user at the first site 1004 is then presented with, for example, an order form for purchasing the product represented by the object 1006.

It will be appreciated that the creators of objects 1006 having embedded URL addresses or indices (which objects may be referred to as "hot objects") and the manufacturers hoping to advertise their goods and services can now spread their creative content like dandelion seeds in the wind across the WWW, knowing that embedded within those seeds are links back to their own home page.

It is contemplated that the object 1006 may include a visible icon 1012 (such as the exemplary "HO" abbreviation shown in Fig. 27) incorporated as part of the graphic. The icon or other subtle indicia would apprise the user that the object is a hot object, carrying the embedded URL address or other information that is accessible via the software 1010.

Any human-perceptible indicium (e.g., a short musical tone) can serve the purpose of apprising the user of the hot object. It is contemplated, however, that no such indicium is required. A user's trial-and-error approach to clicking on a data object having no embedded address will merely cause the software to look for, but not find, the URL address.

The automation process inherent in the use of this aspect of the technology is very advantageous. Web software and web site development tools simply need to recognize this new class of embedded hot links (hot objects), operating on them in real time. Conventional hot links can be modified and supplemented simply by "uploading" a hot object into a web site repository, never requiring a web site programmer to do a thing other than basic monitoring of traffic.

A method of implementing the above described functions of the present technology generally involves the steps of (1) creating a set of standards by which URL addresses are steganographically embedded within images, video, audio, and other forms of data objects; and (2) designing web site development tools and web software such that they recognize this new type of data object (the hot object), the tools being designed such that when the objects are presented to a user and that user points and clicks on such an object, the user's software knows how to read or decode the steganographic information and route the user to the decoded URL address.

The foregoing portions of this description detailed a steganographic implementation (see, generally, Fig. 2 and the text associated therewith) that is readily adapted to implement the present technology. In this regard, the otherwise conventional site development tool 1008 is enhanced to include, for example, the capability to encode a bit-mapped image file with an identification code (URL address, for example) according to the present technology. In the present embodiment, it is contemplated that the commercial or transaction based hot objects may be steganographically embedded with URL addresses (or other information) using any of the universal codes described above.

The foregoing portions of this description also detailed a technique for reading or decoding steganographically embedded information (see, generally, Fig. 3 and the text associated therewith) that is readily adapted to implement the present technology. In this regard, the otherwise conventional user software 1010 is enhanced to include, for example, the capability to analyze encoded bit-mapped files and extract the identification code (URL address, for example).

While an illustrative implementation for steganographically embedding information on a data object has been described, one of ordinary skill will appreciate that any one of the multitude of available steganographic techniques may be employed to carry out the function of the present embodiment.

It will be appreciated that the present embodiment provides an immediate and common sense mechanism whereby some of the fundamental building blocks of the WWW, namely images and sound, can also become hot links to other web sites. Also, the programming of such hot objects can become fully automated merely through the distribution and availability of images and audio. No real web site programming is required. The present embodiment provides for the commercial use of the WWW in such a way that non-programmers can easily spread their message merely by creating and distributing creative content (herein, hot objects). As noted, one can also transition web based hot links themselves from a more arcane text based interface to a more natural image based interface.

Encapsulated Hot Link File Format

As noted above, once steganographic methods of hot link navigation take hold, then, as new file formats and transmission protocols develop, more traditional methods of "header-based" information attachment can enhance the basic approach built by a steganographic-based system. One way to begin

extending the steganographic based hot link method back into the more traditional header-based method is to define a new class of file format which could effectively become the standard class used in network navigation systems. It will be seen that objects beyond images, audio and the like can now become "hot objects", including text files, indexed graphic files, computer programs, and the like.

The encapsulated hot link (EHL) file format simply is a small shell placed around a large range of pre-existing file formats. The EHL header information takes only the first N bytes of a file, followed by a full and exact file in any kind of industry standard format. The EHL super-header merely attaches the correct file type, and the URL address or other index information associating that object to other nodes on a network or other databases on a network.

It is possible that the EHL format could be the method by which the steganographic methods are slowly replaced (but probably never completely). The slowness pays homage to the idea that file format standards often take much longer to create, implement, and get everybody to actually use (if at all). Again, the idea is that an EHL-like format and system built around it would bootstrap onto a system setup based on steganographic methods.

Self Extracting Web Objects

Generally speaking, three classes of data can be steganographically embedded in an object: a number (e.g. a serial or identification number, encoded in binary), an alphanumeric message (e.g. a human readable name or telephone number, encoded in ASCII or a reduced bit code), or computer instructions (e.g. JAVA or HTML instructions). The embedded URLs and the like detailed above begin to explore this third class, but a more detailed exposition of the possibilities may be helpful.

Consider a typical web page, shown in Fig. 27A. It may be viewed as including three basic components: images (#1 - #6), text, and layout.

Applicant's technology can be used to consolidate this information into a self-extracting object, and regenerate the web page from this object.

In accordance with this example, Fig. 27B shows the images of the Fig. 27A web page fitted together into a single RGB mosaiced image. A user can perform this operation manually using existing image processing programs, such as Adobe's Photoshop software, or the operation can be automated by a suitable software program.

Between certain of the image tiles in the Fig. 27B mosaic are empty areas (shown by cross-hatching).

This mosaiced image is then steganographically encoded to embed the layout instructions (e.g. HTML) and the web page text therein. In the empty areas the encoding gain can be maximized since there is no image data to corrupt. The encoded, mosaiced image is then JPEG compressed to form a self extracting web page object.

(JPEG compression is used in this example as a *lingua franca* of image representations. Another such candidate is the GIF file format. Such formats are supported by a variety of software tools and languages, making them well suited as "common carriers" of embedded information. Other image representations can of course be used.)

These objects can be exchanged as any other JPEG images. When the JPEG file is opened, a suitably programmed computer can detect the presence of the embedded information and extract the layout data and text. Among other information, the layout data specifies where the images forming the mosaic are to be located in the final web page. The computer can follow the embedded HTML instructions to recreate the original web page, complete with graphics, text, and links to other URLs.

If the self extracting web page object is viewed by a conventional JPEG viewer, it does not self-extract. However, the user will see the logos and artwork associated with the web page (with noise-like "grouting" between certain of the images). Artisans will recognize that this is in stark contrast to viewing of other compressed data objects (e.g. PKZIP files and self extracting text archives) which typically appear totally unintelligible unless fully extracted.

(The foregoing advantages can largely be achieved by placing the web page text and layout instructions in a header file associated with a JPEG-compressed mosaiced image file. However, industry standardization of the header formats needed to make such systems practical appears difficult, if not impossible.)

Palettes of Steganographically Encoded Images

Once web images with embedded URL information become widespread, such web images can be collected into "palettes" and presented to users as high level navigation tools. Navigation is effected by clicking on such images (e.g. logos for different web pages) rather than clicking on textual web page names. A suitably programmed computer can decode the embedded URL information from the selected image, and establish the requested connection.

In one embodiment, self-extraction of the above-described web page objects automatically generates thumbnail images corresponding to the extracted pages (e.g. representative logos), which are then stored in a subdirectory in the computer's file system dedicated to collecting such thumbnails. In each such thumbnail is embedded a URL, such as the URL of the extracted page or the URL of the site from which the self-extracting object was obtained. This subdirectory can be accessed to display a palette of navigational thumbnails for selection by the user.

Specific Example of a Computer System Linked by Using Information in Data Objects

The present invention allows a digital watermark to be embedded directly into photographs, video, computer images, audio, and other forms of creative property. The range of applications is amazingly

wide, and includes things like video and movie content watermarking for proof of ownership and tracking, watermarking music and audio content, even texturing physical materials such as auto parts. As discussed above, this watermark is imperceptible to the eye, and imperceptible to the ear, but a computer analysis can read the watermark and discover a message it carries. The watermark is repeated throughout the property. It is robust, and typically survives multiple generations of copying, modification, printing, scanning, and compression. A watermark may carry a copyright notice, a unique serial number, a Transaction ID, as well as other application specific data.

Conceptually, the example below is made with respect to a watermark embedded by "PictureMarc" which illustrates the idea by carrying a unique creator id, and a set of image attributes. This creator id corresponds to complete contact information available through an on-line service, MarcCentre. Technically, the watermark is 128 bits long and has a data payload of 76 bits, although the invention is not restricted to any particular watermark size. In this example, it is short so that it can be repeated many times through an image, making it possible to find the message even from a portion of the original image. Other approaches can include data such as an image serial number or a Transaction ID in the watermark message. It is also possible to add a person's name or other such data (to a computer, it is all data), but one application is focused on embedding a more structured message. First, to accommodate a text string, there would be a tendency to push for longer messages. Long messages result in not being able to fit very many copies of the message in an image, and thus the watermark becomes less robust. Also, just putting a name in an image is much like the credit line in a magazine: A. Jones tells who the person is, but not how to contact the person. With a watermark system available on line, a user can get complete and up to date contact details from each Creator ID through the on-line service. Accordingly, it is preferable to associate persistent digital information with an image. The core software has been designed to enable working with vendors or large customers who may want to develop specific watermark message types for special applications such as embedding the film speed and exposure in the image, or serializing images in a large collection for internal tracking and management.

One approach to implementing this embodiment involves "PictureMarc", which includes a writer portion to embed watermarks and a reader portion to find them and read their contents. This bundle is integrated into Adobe Photoshop® 4.0 (Adobe Photoshop is a trademark of Adobe Systems, Inc.) as a plugin extension, and from the end-user's perspective is free. A free reader will also be available through a web site. PictureMarc for Photoshop is supported on Apple

Macintosh and Microsoft Windows platforms. PictureMarc supports embedding a Creator ID and image attributes in an image. PictureMarc also has the ability to carry a unique Image ID or even a Transaction ID in the watermark. These formats will support tracking images both to a collection, and to the person and terms that were in place when the image sold. The watermark reader will accept and read all watermark formats.

As an example, the first step is to read an image from a CD-ROM, download a file to a local computer over the Internet or convert a hardcopy image, such as a photograph, into digital by scanning the image with any of the common image scanners.. Then start an image manipulation program that supports watermarking, and load the image file from a file selection menu. Select the menu item to add a watermark, and save the watermarked image into a file.

To recover a watermarked image from a digital image on, say, a PC, just as in the case of embedding a watermark, convert the image to a suitable computer file format, scanning it in if needed. Then start either an image manipulation tool supporting watermarking, or start a stand-alone reader. Now open the image. In the case of a preferred embodiment image manipulation tool, the tool will automatically check for a watermark when the digital image file is opened, copied to the system clipboard or the image is scanned into the computer. If present, a copyright symbol is added to the title or status bar, or some other signal is provided to the user. By selecting a read watermark menu option, a user can discover the contents of the watermark. From the results dialog, a user can click on the Web Lookup button to retrieve complete contact information from MarcCentre, a network WWW on-line service. The application can be carried out with at least two kinds of watermarks. The first is a public watermark, which can be read by any suitably configured reader. This is the type of watermark supported by PictureMarc--Its purpose is communication. The second is a private watermark. Private watermarks are associated with a secret key used at the time the watermark is embedded in an image. Only the person with the secret key can find and read a private watermark. Private watermarks are used in proof of ownership applications. Both a public and a private watermark can coexist in an image.

If a user attempts to read a watermark and none is there, the reader portion will simply report that a watermark was not found in the image. If a user attempts to watermark an image already watermarked, the user will be informed there is already a watermark in the image, and

will be prevented from adding another watermark. In creating a composite image, the user is first told about the presence of a watermark in each watermarked original (assuming the use of a tool supporting watermarks). This addresses the first order problem of communicating copyright. The watermark will not prevent creating a composite work, in that a watermarked image, or a portion thereof, can be used as an element of a composite image. However, if the composite image contains multiple watermarked elements, the reader portion will tend to read the watermark from the most dominant piece. However, if the user suspects a component to be watermarked, or is simply interested in the source of an image element, the user can check for the watermark in that element by highlighting the area in question, and invoking the read watermark function. This provides a tool to inspect work to discover sources of individual elements. Copyright hierarchies in composited works and partnering with companies addressing rights management can all be handled in such a network application of a watermark.

Preferably, applications which include watermarking, such as Photoshop 4.0, support automatic detection ("autodetect"). This means that whenever an image is opened or scanned into the application, a quick check is done to determine if a watermark is present. If it is present, a visual indication, such as a copyright symbol, is added to the title or status bar.

The watermark placed by PictureMarc is a 128 bits long, with a data payload of 76 bits. The remaining bits are dedicated to header and control information, and error detection and correction. However, the bandwidth can be increased and consequently the data payload can also be increased. The detect process looks for the presence of a watermark, which completes in a couple of seconds, usually under 3 seconds regardless of image size, and the typical time to perform a full read watermark operation is under 15 seconds.

PictureMarc supports all the file formats of the host application, since it works with pixels in each of the major color schemes (CMYK, RGB, LAB, Grayscale). In the case of PictureMarc for Photoshop, all of the Photoshop file formats are supported.

Note that the watermark itself carries version and message type information, much like a communications message. PictureMarc has been designed to support upward compatibility. Any

suitably configured reader will be able to read previous versions of the watermark. If a reader finds a newer version watermark which it does not support, the user will be notified and told to download the most recent reader.

In the present application of PictureMarc, an image generally needs to be at least 256x256 pixels to carry a watermark. Often a watermark can be found in patches as small as 100 pixels square. Arbitrarily large images can be watermarked, constrained only by available memory and disk space. The watermark does not add data to the image file, since it only makes very small changes to the luminance of pixels. This can change the size of a compressed image by a few percent, but the size of uncompressed images, such as bitmaps (.BMPs), are unchanged. While a watermark survives compression, to watermark an already compressed image, it is preferable to either work from the original, or uncompress, watermark, and recompress the image. Future versions will likely support adding watermarks directly to the JPEG compressed file.

PictureMarc supports the automation features provided by Adobe Photoshop 4.0. This means that repetitive watermarking operations can be automated now. In other applications, support can be provided for unattended batch processing of images, aimed to support the needs of image distributors, especially those companies looking to watermark images as they are distributed with unique Transition IDs.

As to the use of a network on line service, an image creator or distributor subscribes to the MarcCentre, on-line locator service. Subscribing includes providing a set of contact information to be made available when one of a user's watermarked images is found. Contact details include name, address, phone number, specialty, intermediary (e.g., organization, stock agency, representative, etc.) representing the creator's work and so on. When subscribing, the user is given a unique Creator ID. The user provides this Creator ID to a copy of PictureMarc, one time when first using the software-based system. This Creator ID links all of the user's images to facilitate contact details. Information can be queried via the Internet, or via a fax-back service. Querying is preferably free.

A subscription to MarcCentre is priced to include unlimited access to contact information by anyone finding watermarked images. A Creator ID in the image leverages the power of a network accessible database, and lets the image creator communicate much more information than could fit in the image. In essence, we are creating a copyright communication system. Watermark detection in programs such as Photoshop is automatic. The Creator ID in the image, along with the image attributes, uniquely identify the image creator or distributor. The contact information corresponding to the Creator ID is always up to date, no matter how long ago a watermarked image was distributed. To make this copyright communication system work, we need unique ids which correspond to the appropriate image creator contact information.

If there is no network connection for PictureMarc, an equivalent approach can be used: contact information can be communicated via a fax-back service. This can be carried out by punching in the Creator ID on a touch-tone keypad with telephony, and the resulting contact details for that image creator will be sent by fax.

Contact details will be stored on a robust server being hosted by an Internet provider. The Web site is responsible for maintaining the locator service and ensuring that information is available. Individual image creators are responsible for maintaining their own contact details, keeping them current as information changes. This ensures that all of the images distributed point to up-to-date information about the creator and the creator's work.

Data in the Web site repository is stored in a way that when a user enter contact details, the user has control over which pieces of information are viewable by viewers. Thus, for example, the user can designate whether to exclude his or her address, phone number, and other specific information.

It is helpful for users to receive regular reports, generated by the Web page site software, about the number of people querying a specific user's information. These can be sent to the user via e-mail or fax, to help communicate the activity concerning watermarked images.

Before turning to a specific embodiment of the present invention, it is important to stress the general applicability of embedding a watermark, then reading it to obtain data, and then using the data to link to a database--preferably via a computer network. This is applicable to all media for which this technology is useful. This includes watermarking a photograph or a series of watermarks in a series of images (e.g., television, video), in sound or other analog signals (e.g., recordings, cellular telephone or other broadcasts), and other applications indicated herein. In any of these applications, while the watermark can contain self-identifying data, a centralized repository of watermark data facilitates broad, efficient usage.

Thus, the following specific description of a preferred embodiment of a central repository, accessible by a network, is intended to be illustrative of the same kind of an approach for other applications and media suitable for watermarking. And it is to be understood that while the following discussion is made in the context of image processing, the same general approach can be used for handling watermarks in acoustic or other applications. Also, while the Adobe Photoshop application is used to illustrate the generally applicable concepts, it should be appreciated that the present invention can be used in connection with other such products from other vendors, as well as in stand alone form.

Fig. 43 illustrates an application of the invention using such an application as Adobe Photoshop 4.0, equipped with a plug in version of the digital watermarking technology discussed herein and illustrated as "PictureMarc," running on a digital electrical computer. The computer running the Adobe application is adapted for communication over a network (such as the WWW) with another digital electrical computer, running the MarcCentre Web Page computer program.

At step 1 of Fig. 43 a creator of a digitized photographic image, the "user" of the Adobe Photoshop, commences by obtaining a Creator ID. Such data is created and stored in a central repository designated in Fig. 43 as MarcCentre Locator Service, which is connectable to PictureMarc via Internet or fax. At step 2 of Fig. 43, the user creates and embeds a watermark in the digital image. At step 3 of Fig. 43, that image can be stored and/or printed, possibly subsequent to distribution over a computer system such as the Internet or WWW. When the image bearing the watermark is used in digital form, at step 4 of Fig. 43, that image is examined

for a watermark by a computer running the PictureMarc computer program. Preferably, the examination is conducted automatically (rather than selectively) upon opening an image, e.g., upon locating the image on a computer screen clipboard. If a watermark is detected, at step 5 of Fig. 43, PictureMarc communicates with the MarcCentre Locator Service to look up creator information and present a WWW page to the user.

The means by which a user obtains a Creator ID in step 1 of Fig. 43 is elaborated in Figs. 44, 45, and 46, which represent screen images of MarcCentre, a Web Page locatable on the WWW. Introductory information is set forth in Fig. 44. Note the mention of a single mouse click. This feature refers to a hot button, such as a copyright symbol in a title bar of a screen, which permits someone using the Web Page to obtain information about the image that was pre-specified by the creator. (A hot button (pointer to information stored in a MarcCentre database, which can in turn have a pointer to another database, such as that accessed by means of the network or WWW.)

Figs. 45 and 46 show sequential screens of a "form" to be completed by computer entries. This information is stored in a MarcCentre database. Note too that the information entered to complete the form include a fee, and the fee account for the user is also stored in a MarcCentre database. After the form has been completed and stored and the fee has been secured, a Creator ID is issued by the MarcCentre service.

The means by which a user with a Creator ID embeds a registered watermark in step 2 of Fig. 43 is elaborated in Figs. 47, 48, and 49. The Photoshop software uses a filter to call up the "Digimarc" PictureMarc software and select options to embed a watermark. Bolded bars on the screen of Fig. 47 illustrate a selection being made for a digital image in the background. Other information on the screen is typical for a windows application, the Adobe Photoshop application, and or generally known information about digital images, e.g., 100% shows the scale of the image, "RGB" indicates the image format, etc.

Fig. 48 illustrates a "Dialog Box" used in associating information in connection with the embedding of the watermark. In a portion of the screen, the Copyright Information is

specified, including the Creator ID, the Type of Use (either Restricted or Royalty Free), Adult Content, and a Personalize option. A demonstration ID for use by those who do not have a registered Creator ID is "PictureMarc Demo." The Adult Content feature permits embedding in the watermark data, preferably content-indicative data. Here the data is used for identifying that the photograph contains adult content, and thus a subsequent use of the photograph can be restricted. However, an alternative is to include other data or other content-identifying data, such as cataloging information, in the watermark itself. Cataloging information permits subject matter searching in a collection of photographs. Another feature shown in Fig. 48 is a slidable scale for adjusting the intensity of the watermark. The more visible the watermark, the more durable the watermark is. Watermark durability (visibility) is also indicated by a number shown on the screen. Once the screen has been completed, if it is "OK", the user can click on this button and thereby embed the watermark. Otherwise, the user can select to cancel and thereby abort the process that would have led to the watermarking.

Selecting the Personalize option of Fig. 48 calls the screen illustrated in Fig. 49, which is used to obtain a personalized, registered Creator ID. After the Creator ID is entered, selection of the Register option launches a WWW browser directed by the URL address shown entered on the screen to the MarcCentre registration page.

In a preferred embodiment of step 4 of Fig. 43, each time an image is opened, scanned in, or copied to the clipboard by any application, the image is automatically tested for a watermark, as illustrated in Fig. 50. This "autodetect" approach generates a signal indicative of the result of the test, for example, one or more copyright symbols shown in the title page of the screen in Fig. 50. Automatic checking for a watermark takes less computer time than the alternative of selectively reading the watermark, which is illustrated in Figs. 51 and 52. However, the selective approach is less comprehensive in monitoring the use of watermarked images, which is disadvantageous if the application is configured to automatically report the detection back to the MarcCentre. In Fig. 50, the copyright symbol in the title area of the photograph is the previously mentioned hot button. The copyright symbol in the lower left of the screen can alternatively or also be a hot button.

Figs. 51 and 52 elaborate the alternative approach to step 4 of Fig. 43 in which an image is opened and examined for a watermark. Preferably, each time an image is opened, there is an automatic check for a watermark. In any case, Fig. 51 is similar to the screen of Fig. 47, except that a selection is shown to read for a watermark.

Fig. 52 shows a screen that is be produced in response to the reading a watermark. This screen provides the Creator ID of the owner and / or distributor of this image, as well as whether use of this image is restricted or royalty free. Note the Web Lookup button, which can be selected to launch a WWW browser directed by the URL address shown entered on the screen to the MarcCentre Web Page, and obtains the data in the corresponding MarcCentre database corresponding to the Creator ID.

Fig. 53 illustrates a screen produced from selecting the Web Lookup feature of Fig. 53. This screen provides the contact information for the image creator, including phone number, E-mail address and Web links. Note the selectable buttons at the bottom of the screen illustrated in Fig. 53, including buttons that take the user to promotional offers, allow the user to download additional software, subscribe to the MarcCentre service, update contact information, search for a creator or provide feedback on the MarcCentre service. Selecting the Creator Search option leads to the screen shown in Fig. 54 This self-explanatory screen enables a user to obtain contact information about a particular creator by entering the Creator ID.

In a variation on the above-described approach, extended information is embedded in the watermark and subsequently detected, as respectively illustrated in Figs.' 55 and 56. Such a feature would be inserted as an additional filter in Fig. 47. In Fig. 55., the dialog box permits inputting an Organization ID, an Item ID, and a Transaction ID. An Organization ID identifies an organization or other intermediary representing the creator and/or authorized for distributing the photograph and licensing rights thereto, such as a photo stock house. An Item ID identifies the photograph in a collection, such as a CD ROM. A Transaction ID identifies the specific transaction that is authorized (e.g., publication one time only in a newspaper), which permits detection of an authorized usage. The other feature on the screen, The Bump Size specification, pertains to the smallest unit of data, in the horizontal and vertical directions, that the watermark algorithms operate on. The extended information embedded in the watermark can be detected in

a manner analogous to that described with respect to Fig. 48, except that the additional information is shown as illustrated in Fig. 56.

An alternative to a "plug in" embodiment is a stand alone version, which is exemplified in the next sequence of figures. As discussed above, for any application that involves a watermark, preferably there is an autodetect capability, and Fig. 57 illustrates a screen from a stand alone image reader with a clip board triggered by merely putting an image on the clipboard. In the Clipboard Viewer window of Fig. 57, a watermark detected on the image can be used to signal the user by one of several methods that can be used individually or in a combination. In one method, a title bar icon or some other bar or icon alternates between "normal" and "watermark detected" states periodically (for example, at one second intervals). Another approach is to use other state changes, like having the title bar or a task bar alternate between highlighted and normal states periodically. Still another method is to have the detection initiate a special dialog box display, as illustrated in Fig. 58. The Read button in the special dialog box (triggered by a click of a mouse, like other buttons) causes reading and display of the watermark information in the image. The Close button ends the special dialog. (So as not to interfere with image processing, it can be convenient to show the special dialog box for a limited amount of time, and a small window therein can show the time remaining before the special dialog box disappears.) Buttons shown on the screen include one resembling a file folder to open a file; the next button is for copying a selected image from a first application to the clipboard; the next button is for pasting an image from the clipboard to a second application; and the last is for help menus.

Fig. 59 shows the image after pasting it from the clipboard, in the course of image processing. The Digimarc Reader - Image 1 window pops up on the screen to permit clicking the Web lookup button, which launches the user's web browser to result in a display of the creator's web page on the MarcCentre Web site, with the rest following as above.

Note again that the foregoing approach is representative, and it can be modified for another media in which a watermark is used. For example, instead of an image, a sound can be used.

POTENTIAL USE OF THE TECHNOLOGY IN THE PROTECTION AND CONTROL OF SOFTWARE PROGRAMS

The illicit use, copying, and reselling of software programs represents a huge loss of revenues to the software industry at large. The prior art methods for attempting to mitigate this problem are very broad and will not be discussed here. What will be discussed is how the principles of this technology might be brought to bear on this huge problem. It is entirely unclear whether the tools provided by this technology will have any economic advantage (all things considered) over the existing countermeasures both in place and contemplated.

The state of technology over the last decade or more has made it a general necessity to deliver a full and complete copy of a software program in order for that program to function on a user's computer. In effect, $X were invested in creating a software program where X is large, and the entire fruits of that development must be delivered in its entirety to a user in order for that user to gain value from the software product. Fortunately this is generally compiled code, but the point is that this is a shaky distribution situation looked at in the abstract. The most mundane (and harmless in the minds of most perpetrators) illicit copying and use of the program can be performed rather easily.

This disclosure offers, at first, an abstract approach which may or may not prove to be economical in the broadest sense (where the recovered revenue to cost ratio would exceed that of most competing methods, for example). The approach expands upon the methods and approaches already laid out in the section on plastic credit and debit cards. The abstract concept begins by positing a "large set of unique patterns," unique among themselves, unique to a given product, and unique to a given purchaser of that product. This set of patterns effectively contains thousands and even millions of absolutely unique "secret keys" to use the cryptology vernacular. Importantly and distinctly, these keys are non-deterministic, that is, they do not arise from singular sub-1000 or sub-2000 bit keys such as with the RSA key based systems. This large set of patterns is measured in kilobytes and Megabytes, and as mentioned, is non-deterministic in

nature. Furthermore, still at the most abstract level, these patterns are fully capable of being encrypted via standard techniques and analyzed within the encrypted domain, where the analysis is made on only a small portion of the large set of patterns, and that even in the worst case scenario where a would-be pirate is monitoring the step-by-step microcode instructions of a microprocessor, this gathered information would provide no useful information to the would-be pirate. This latter point is an important one when it comes to "implementation security" as opposed to "innate security" as will be briefly discussed below.

So what could be the differential properties of this type of key based system as opposed to, for example, the RSA cryptology methods which are already well respected, relatively simple, etc. etc? As mentioned earlier, this discussion is not going to attempt a commercial side-by-side analysis. Instead, we'll just focus on the differing properties. The main distinguishing features fall out in the implementation realm (the implementation security). One example is that in single low-bit-number private key systems, the mere local use and re-use of a single private key is an inherently weak link in an encrypted transmission system. ["Encrypted transmission systems" are discussed here in the sense that securing the paid-for use of software programs will in this discussion require de facto encrypted communication between a user of the software and the "bank" which allows the user to use the program; it is encryption in the service of electronic financial transactions looked at in another light.] Would-be hackers wishing to defeat so-called secure systems never attack the fundamental hard-wired security (the innate security) of the pristine usage of the methods, they attack the implementation of those methods, centered around human nature and human oversights. It is here, still in the abstract, that the creation of a much larger key base, which is itself non-deterministic in nature, and which is more geared toward effectively throw-away keys, begins to "idiot proof" the more historically vulnerable implementation of a given secure system. The huge set of keys is not even comprehensible to the average holder of those keys, and their use of those keys (i.e., the "implementation" of those keys) can randomly select keys, easily throw them out after a time, and can use them in a way that no "eavesdropper" will gain any useful information in the eavesdropping, especially when well within a millionth of the amount of time that an eavesdropper could "decipher" a key, its usefulness in the system would be long past.

Turning the abstract to the semi-concrete, one possible new approach to securely delivering a software product to ONLY the bonafide purchasers of that product is the following. In a mass economic sense, this new method is entirely founded upon a modest rate realtime digital connectivity (often, but not necessarily standard encrypted) between a user's computer network and the selling company's network. At first glance this smells like trouble to any good marketing person, and indeed, this may throw the baby out with the bathwater if by trying to recover lost revenues, you lose more legitimate revenue along the way (all part of the bottom line analysis). This new method dictates that a company selling a piece of software supplies to anyone who is willing to take it about 99.8% of its functional software for local storage on a user's network (for speed and minimizing transmission needs). This "free core program" is entirely unfunctional and designed so that even the craftiest hackers can't make use of it or "decompile it" in some sense. Legitimate activation and use of this program is performed purely on a instruction-cycle-count basis and purely in a simple very low overhead communications basis between the user's network and the company's network. A customer who wishes to use the product sends payment to the company via any of the dozens of good ways to do so. The customer is sent, via common shipment methods, or via commonly secured encrypted data channels, their "huge set of unique secret keys." If we were to look at this large set as if it were an image, it would look just like the snowy images discussed over and over again in other parts of this disclosure. (Here, the "signature" is the image, rather than being imperceptibly placed onto another image). The special nature of this large set is that it is what we might call "ridiculously unique" and contains a large number of secret keys. (The "ridiculous" comes from the simple math on the number of combinations that are possible with, say 1 Megabyte of random bit values, equaling exactly the number that "all ones" would give, thus 1 Megabyte being approximately 10 raised to the ~2,400,000 power, plenty of room for many people having many throwaway secret keys). It is important to re-emphasize that the purchased entity is literally: productive use of the tool. The marketing of this would need to be very liberal in its allotment of this productivity, since per-use payment schemes notoriously turn off users and can lower overall revenues significantly.

This large set of secret keys is itself encrypted using standard encryption techniques. The basis for relatively higher "implementation security" can now begin to manifest itself. Assume that the user now wishes to use the software product. They fire up the free core, and the free

core program finds that the user has installed their large set of unique encrypted keys. The core program calls the company network and does the usual handshaking. The company network, knowing the large set of keys belonging to that bonafide user, sends out a query on some simple set of patterns, almost exactly the same way as described in the section on the debit and credit cards. The query is such a small set of the whole, that the inner workings of the core program do not even need to decrypt the whole set of keys, only certain parts of the keys, thus no decrypted version of the keys ever exist, even within the machine cycles on the local computer itself. As can be seen, this does not require the "signatures within a picture" methods of the main disclosure, instead, the many unique keys ARE the picture. The core program interrogates the keys by performing certain dot products, then sends the dot products back to the company's network for verification. See Fig. 25 and the accompanying discussion for typical details on a verification transaction. Generally encrypted verification is sent, and the core program now "enables" itself to perform a certain amount of instructions, for example, allowing 100,000 characters being typed into a word processing program (before another unique key needs to be transmitted to enable another 100,000). In this example, a purchaser may have bought the number of instructions which are typically used within a one year period by a single user of the word processor program. The purchaser of this product now has no incentive to "copy" the program and give it to their friends and relatives.

All of the above is well and fine except for two simple problems. The first problem can be called "the cloning problem" and the second "the big brother problem." The solutions to these two problems are intimately linked. The latter problem will ultimately become a purely social problem, with certain technical solutions as mere tools not ends.

The cloning problem is the following. It generally applies to a more sophisticated pirate of software rather than the currently common "friend gives their distribution CD to a friend" kind of piracy. Crafty-hacker "A" knows that if she performs a system-state clone of the "enabled" program in its entirety and installs this clone on another machine, then this second machine effectively doubles the value received for the same money. Keeping this clone in digital storage, hacker "A" only needs to recall it and reinstall the clone after the first period is run out, thus indefinitely using the program for a single payment, or she can give the clone to their hacker friend "B" for a six-pack of beer. One good solution to this problem requires, again, a rather well

developed and low cost real time digital connectivity between user site and company enabling network. This ubiquitous connectivity generally does not exist today but is fast growing through the Internet and the basic growth in digital bandwidth. Part and parcel of the "enabling" is a negligible communications cost random auditing function wherein the functioning program routinely and irregularly performs handshakes and verifications with the company network. It does so, on average, during a cycle which includes a rather small amount of productivity cycles of the program. The resulting average productivity cycle is in general much less than the raw total cost of the cloning process of the overall enabled program. Thus, even if an enabled program is cloned, the usefulness of that instantaneous clone is highly limited, and it would be much more cost effective to pay the asking price of the selling company than to repeat the cloning process on such short time periods. Hackers could break this system for fun, but certainly not for profit. The flip side to this arrangement is that if a program "calls up" the company's network for a random audit, the allotted productivity count for that user on that program is accounted for, and that in cases where bonafide payment has not been received, the company network simply withholds its verification and the program no longer functions. We're back to where users have no incentive to "give this away" to friends unless it is an explicit gift (which probably is quite appropriate if they have indeed paid for it: "do anything you like with it, you paid for it").

The second problem of "big brother" and the intuitively mysterious "enabling" communications between a user's network and a company's network would as mentioned be a social and perceptual problem that should have all manner of potential real and imagined solutions. Even with the best and objectively unbeatable anti-big-brother solutions, there will still be a hard-core conspiracy theory crowd claiming it just ain't so. With this in mind, one potential solution is to set up a single program registry which is largely a public or non-profit institution to handling and coordinating the realtime verification networks. Such an entity would then have company clients as well as user clients. An organization such as the Software Publishers Association, for example, may choose to lead such an effort.

Concluding this section, it should be re-emphasized that the methods here outlined require a highly connected distributed system, in other words, a more ubiquitous and inexpensive Internet than exists in mid 1995. Simple trend extrapolation would argue that this is not too far off from

1995. The growth rate in raw digital communications bandwidth also argues that the above system might be more practical, sooner, than it might first appear. (The prospect of interactive TV brings with it the promise of a fast network linking millions of sites around the world.)

USE OF CURRENT CRYPTOLOGY METHODS IN CONJUNCTION WITH THIS TECHNOLOGY

It should be briefly noted that certain implementations of the principles of this technology probably can make good use of current cryptographic technologies. One case in point might be a system whereby graphic artists and digital photographers perform realtime registration of their photographs with the copyright office. It might be advantageous to send the master code signals, or some representative portion thereof, directly to a third party registry. In this case, a photographer would want to know that their codes were being transmitted securely and not stolen along the way. In this case, certain common cryptographic transmission might be employed. Also, photographers or musicians, or any users of this technology, may want to have reliable time stamping services which are becoming more common. Such a service could be advantageously used in conjunction with the principles of this technology.

DETAILS ON THE LEGITIMATE AND ILLEGITIMATE DETECTION AND REMOVAL OF INVISIBLE SIGNATURES

In general, if a given entity can recognize the signatures hidden within a given set of empirical data, that same entity can take steps to remove those signatures. In practice, the degree of difficulty between the former condition and the latter condition can be made quite large, fortunately. On one extreme, one could posit a software program which is generally very difficult to "decompile" and which does recognition functions on empirical data. This same bit of software could not generally be used to "strip" the signatures (without going to extreme lengths).

On the other hand, if a hacker goes to the trouble of discovering and understanding the "public codes" used within some system of data interchange, and that hacker knows how to recognize the signatures, it would not be a large step for that hacker to read in a given set of signed data and create a data set with the signatures effectively removed. In this latter example, interestingly enough, there would often be telltale statistics that signatures had been removed, statistics which will not be discussed here.

These and other such attempts to remove the signatures we can refer to as illicit attempts. Current and past evolution of the copyright laws have generally targeted such activity as coming under criminal activity and have usually placed such language, along with penalties and enforcement language, into the standing laws. Presumably any and all practitioners of this signature technology will go to lengths to make sure that the same kind of a) creation, b) distribution, and c) use of these kinds of illicit removal of copyright protection mechanisms are criminal offenses subject to enforcement and penalty. On the other hand, it is an object of this technology to point out that through the recognition steps outlined in this disclosure, software programs can be made such that the recognition of signatures can simply lead to their removal by inverting the known signatures by the amount equal to their found signal energy in the recognition process (i.e., remove the size of the given code signal by exact amount found). By pointing this out in this disclosure, it is clear that such software or hardware which performs this signature removal operation will not only (presumably) be criminal, but it will also be liable to infringement to the extent that it is not properly licensed by the holders of the (presumably) patented technology.

The case of legitimate and normal recognition of the signatures is straightforward. In one example, the public signatures could deliberately be made marginally visible (i.e. their intensity would be deliberately high), and in this way a form of sending out "proof comps" can be accomplished. "Comps" and "proofs" have been used in the photographic industry for quite some time, where a degraded image is purposely sent out to prospective customers so that they might evaluate it but not be able to use it in a commercially meaningful way. In the case of this technology, increasing the intensity of the public codes can serve as a way to "degrade" the commercial value intentionally, then through hardware or software activated by paying a purchase

price for the material, the public signatures can be removed (and possibly replaced by a new invisible tracking code or signature, public and/or private.

MONITORING STATIONS AND MONITORING SERVICES

Ubiquitous and cost effective recognition of signatures is a central issue to the broadest proliferation of the principles of this technology. Several sections of this disclosure deal with this topic in various ways. This section focuses on the idea that entities such as monitoring nodes, monitoring stations, and monitoring agencies can be created as part of a systematic enforcement of the principles of the technology. In order for such entities to operate, they require knowledge of the master codes, and they may require access to empirical data in its raw (unencrypted and untransformed) form. (Having access to original unsigned empirical data helps in finer analyses but is not necessary.)

Three basic forms of monitoring stations fall out directly from the admittedly arbitrarily defined classes of master codes: a private monitoring station, a semi-public, and a public. The distinctions are simply based on the knowledge of the master codes. An example of the fully private monitoring station might be a large photographic stock house which decides to place certain basic patterns into its distributed material which it knows that a truly crafty pirate could decipher and remove, but it thinks this likelihood is ridiculously small on an economic scale. This stock house hires a part-time person to come in and randomly check high value ads and other photography in the public domain to search for these relatively easy to find base patterns, as well as checking photographs that stock house staff members have "spotted" and think it might be infringement material. The part time person cranks through a large stack of these potential infringement cases in a few hours, and where the base patterns are found, now a more thorough analysis takes place to locate the original image and go through the full process of unique identification as outlined in this disclosure. Two core economic values accrue to the stock house in doing this, values which by definition will outweigh the costs of the monitoring service and the cost of the signing process itself. The first value is in letting their customers and the world know

that they are signing their material and that the monitoring service is in place, backed up by whatever statistics on the ability to catch infringers. This is the deterrent value, which probably will be the largest value eventually. A general pre-requisite to this first value is the actual recovered royalties derived from the monitoring effort and its building of a track record for being formidable (enhancing the first value).

The semi-public monitoring stations and the public monitoring stations largely follow the same pattern, although in these systems it is possible to actually set up third party services which are given knowledge of the master codes by clients, and the services merely fish through thousands and millions of "creative property" hunting for the codes and reporting the results to the clients. ASCAP and BMI have "lower tech" approaches to this basic service.

A large coordinated monitoring service using the principles of this technology would classify its creative property supplier clients into two basic categories, those that provide master codes themselves and wish the codes to remain secure and unpublished, and those that use generally public domain master codes (and hybrids of the two, of course). The monitoring service would perform daily samplings (checks) of publicly available imagery, video, audio, etc., doing high level pattern checks with a bank of supercomputers. Magazine ads and images would be scanned in for analysis, video grabbed off of commercial channels would be digitized, audio would be sampled, public Internet sites randomly downloaded, etc. These basic data streams would then be fed into an ever-churning monitoring program which randomly looks for pattern matches between its large bank of public and private codes, and the data material it is checking. A small sub-set, which itself will probably be a large set, will be flagged as potential match candidates, and these will be fed into a more refined checking system which begins to attempt to identify which exact signatures may be present and to perform a more fine analysis on the given flagged material. Presumably a small set would then fall out as flagged match material, owners of that material would be positively identified and a monitoring report would be sent to the client so that they can verify that it was a legitimate sale of their material. The same two values of the private monitoring service outlined above apply in this case as well. The monitoring service could also serve as a formal bully in cases of a found and proven infringement, sending out letters to infringing parties witnessing the found infringement and seeking inflated royalties so that the infringing party might avoid the more costly alternative of going to court.

METHOD FOR EMBEDDING SUBLIMINAL REGISTRATION PATTERNS INTO IMAGES AND OTHER SIGNALS

The very notion of reading embedded signatures involves the concept of registration. The underlying master noise signal must be known, and its relative position needs to be ascertained (registered) in order to initiate the reading process itself (e.g. the reading of the 1's and 0's of the N-bit identification word). When one has access to the original or a thumbnail of the unsigned signal, this registration process is quite straightforward. When one doesn't have access to this signal, which is often the case in universal code applications of this technology, then different methods must be employed to accomplish this registration step. The example of pre-marked photographic film and paper, where by definition there will never be an "unsigned" original, is a perfect case in point of the latter.

Many earlier sections have variously discussed this issue and presented certain solutions. Notably, the section on "simple" universal codes discusses one embodiment of a solution where a given master code signal is known a priori, but its precise location (and indeed, it existence or non-existence) is not known. That particular section went on to give a specific example of how a very low level designed signal can be embedded within a much larger signal, wherein this designed signal is standardized so that detection equipment or reading processes can search for this standardized signal even though its exact location is unknown. The brief section on 2D universal codes went on to point out that this basic concept could be extended into 2 dimensions, or, effectively, into imagery and motion pictures. Also, the section on symmetric patterns and noise patterns outlined yet another approach to the two dimensional case, wherein the nuances associated with two dimensional scale and rotation were more explicitly addressed. Therein, the idea was not merely to determine the proper orientation and scale of underlying noise patterns, but to have information transmitted as well, e.g., the N rings for the N-bit identification word.

This section now attempts to isolate the sub-problem of registering embedded patterns for registration's sake. Once embedded patterns are registered, we can then look again at how this registration can serve broader needs. This section presents yet another technique for embedding patterns, a technique which can be referred to as "subliminal digital graticules". "Graticules" - other words such as fiducials or reticles or hash marks could just as well be used -conveys the

idea of calibration marks used for the purposes of locating and/or measuring something. In this case, they are employed as low level patterns which serve as a kind of gridding function. That gridding function itself can be a carrier of 1 bit of information, as in the universal 1 second of noise (its absence or presence, copy me, don't copy me), or it can simply find the orientation and scale of other information, such as embedded signatures, or it can simply orient an image or audio object itself.

Figs. 29 and 30 visually summarize two related methods which illustrate applicant's subliminal digital graticules. As will be discussed, the method of Fig. 29 may have slight practical advantages over the method outlined in Fig. 30, but both methods effectively decompose the problem of finding the orientation of an image into a series of steps which converge on a solution. The problem as a whole can be simply stated as the following: given an arbitrary image wherein a subliminal digital graticule may have been stamped, then find the scale, rotation, and origin (offset) of the subliminal digital graticule.

The beginning point for subliminal graticules is in defining what they are. Simply put, they are visual patterns which are directly added into other images, or as the case may be, exposed onto photographic film or paper. The classic double exposure is not a bad analogy, though in digital imaging this specific concept becomes rather stretched. These patterns will generally be at a very low brightness level or exposure level, such that when they are combined with "normal" images and exposures, they will effectively be invisible (subliminal) and just as the case with embedded signatures, they will by definition not interfere with the broad value of the images to which they are added.

Figs. 29 and 30 define two classes of subliminal graticules, each as represented in the spatial frequency domain, also known as the UV plane, 1000. Common two dimensional fourier transform algorithms can transform any given image into its UV plane conjugate. To be precise, the depictions in Figs. 29 and 30 are the magnitudes of the spatial frequencies, whereas it is difficult to depict the phase and magnitude which exists at every point.

Fig. 29 shows the example of six spots in each quadrant along the 45 degree lines, 1002. These are exaggerated in this figure, in that these spots would be difficult to discern by visual inspection of the UV plane image. A rough depiction of a "typical" power spectrum of an arbitrary image as also shown, 1004. This power spectrum is generally as unique as images are unique. The subliminal graticules are essentially these spots. In this example, there are six spatial frequencies combined along each of the two 45 degree axes. The magnitudes of the six frequencies can be the same or different (we'll touch upon this refinement later). Generally speaking, the phases of each are different from the others, including the phases of one 45 degree axis relative to the other. Fig. 31 depicts this graphically. The phases in this example are simply randomly placed between PI and -PI, 1008 and 1010. Only two axes are represented in Fig. 31 - as opposed to the four separate quadrants, since the phase of the mirrored quadrants are simply PI/2 out of phase with their mirrored counterparts. If we turned up the intensity on this subliminal graticule, and we transformed the result into the image domain, then we would see a weave-like cross-hatching pattern as related in the caption of Fig. 29. As stated, this weave-like pattern would be at a very low intensity when added to a given image. The exact frequencies and phases of the spectral components utilized would be stored and standardized. These will become the "spectral signatures" that registration equipment and reading processes will seek to measure.

Briefly, Fig. 30 has a variation on this same general theme. Fig. 30 lays out a different class of graticules in that the spectral signature is a simple series of concentric rings rather than spots along the 45 degree axes. Fig. 32 then depicts a quasi-random phase profile as a function along a half-circle (the other half of the circle then being PI/2 out of phase with the first half). These are simple examples and there are a wide variety of variations possible in designing the phase profiles and the radii of the concentric rings. The transform of this type of subliminal graticule is less of a "pattern" as with the weave-like graticule of Fig. 29, where it has more of a random appearance like a snowy image.

The idea behind both types of graticules is the following: embed a unique pattern into an image which virtually always will be quite distinct from the imagery into which it will be added, but which has certain properties which facilitate fast location of the pattern, as well as accuracy properties such that when the pattern is generally located, its precise location and orientation can be found to some high level of precision. A corollary to the above is to design the pattern such

that the pattern on average minimally interferes with the typical imagery into which it will be added, and has maximum energy relative to the visibility of the pattern.

Moving on to the gross summary of how the whole process works, the graticule type of Fig. 29 facilitates an image processing search which begins by first locating the rotation axes of the subliminal graticule, then locating the scale of the graticule, then determining the origin or offset. The last step here identifies which axes is which of the two 45 degree axes by determining phase. Thus even if the image is largely upside down, an accurate determination can be made. The first step and the second step can both be accomplished using only the power spectrum data, as opposed to the phase and magnitude. The phase and magnitude signals can then be used to "fine tune" the search for the correct rotation angle and scale. The graticule of Fig. 30 switches the first two steps above, where the scale is found first, then the rotation, followed by precise determination of the origin. Those skilled in the art will recognize that determining these outstanding parameters, along two axes, are sufficient to fully register an image. The "engineering optimization challenge" is to maximize the uniqueness and brightness of the patterns relative to their visibility, while minimizing the computational overhead in reaching some specified level of accuracy and precision in registration. In the case of exposing photographic film and paper, clearly an additional engineering challenge is the outlining of economic steps to get the patterns exposed onto the film and paper in the first place, a challenge which has been addressed in previous sections.

The problem and solution as above defined is what was meant by registration for registration's sake. It should be noted that there was no mention made of making some kind of value judgement on whether or not a graticule is indeed being found or not. Clearly, the above steps could be applied to images which do not in fact have graticules inside them, the measurements then simply chasing noise. Sympathy needs to be extended to the engineer who is assigned the task of setting "detection thresholds" for these types of patterns, or any others, amidst the incredibly broad range of imagery and environmental conditions in which the patterns must be sought and verified. [Ironically, this is where the pure universal one second of noise stood in a previous section, and that was why it was appropriate to go beyond merely detecting or not detecting this singular signal, i.e. adding additional information planes]. Herein is where some real beauty shows up: in the combination of the subliminal graticules with the now-registered

embedded signatures described in other parts of this disclosure. Specifically, once a "candidate registration" is found - paying due homage to the idea that one may be chasing noise - then the next logical step is to perform a reading process for, e.g., a 64 bit universal code signature. As further example, we can imagine that 44 bits of the 64 bit identification word are assigned as an index of registered users -- serial numbers if you will. The remaining 20 bits are reserved as a hash code - as is well known in encryption arts - on the 44 bit identification code thus found. Thus, in one swoop, the 20 bits serve as the "yes, I have a registered image" or "no, I don't" answer. More importantly, perhaps, this allows for a system which can allow for maximum flexibility in precisely defining the levels of "false positives" in any given automated identification system. Threshold based detection will always be at the mercy of a plethora of conditions and situations, ultimately resting on arbitrary decisions. Give me N coin flips any day.

Back on point, these graticule patterns must first be added to an image, or exposed onto a piece of film. An exemplary program reads in an arbitrarily sized digital image and adds a specified graticule to the digital image to produce an output image. In the case of film, the graticule pattern would be physically exposed onto the film either before, during, or after exposure of the primary image. All of these methods have wide variations in how they might be accomplished.

The searching and registering of subliminal graticules is the more interesting and involved process. This section will first describe the elements of this process, culminating in the generalized flow chart of Fig. 37.

Fig. 33 depicts the first major "search" step in the registration process for graticules of the type in Fig. 29. A suspect image (or a scan of a suspect photograph) is first transformed in its fourier representation using well known 2D FFT routines. The input image may look like the one in Fig. 36, upper left image. Fig. 33 conceptually represents the case where the image and hence the graticules have not been rotated, though the following process fully copes with rotation issues. After the suspect image has been transformed, the power spectrum of the transform is then calculated, being simply the square root of the addition of the two squared moduli. it is also a good idea to perform a mild low pass filter operation, such as a 3x3 blur filter, on the resulting power spectrum data, so that later search steps don't need incredibly fine spaced steps. Then the

candidate rotation angles from 0 through 90 degrees (or 0 to PI/2 in radian) are stepped through. Along any given angle, two resultant vectors are calculated, the first is the simple addition of power spectrum values at a given radius along the four lines emanating from the origin in each quadrant. The second vector is the moving average of the first vector. Then, a normalized power profile is calculated as depicted in both 1022 and 1024, the difference being that one plot is along an angle which does not align with the subliminal graticules, and the other plot does align. The normalization stipulates that the first vector is the numerator and the second vector is the denominator in the resultant vector. As can be seen in Fig. 33, 1022 and 1024, a series of peaks (which should be "six" instead of "five" as is drawn) develops when the angle aligns along its proper direction. Detection of these peaks can be effected by setting some threshold on the normalized values, and integrating their total along the whole radial line. A plot, 1026, from 0 to 90 degrees is depicted in the bottom of Fig. 33, showing that the angle 45 degrees contains the most energy. In practice, this signal is often much lower than that depicted in this bottom figure, and instead of picking the highest value as the "found rotation angle," one can simply find the top few candidate angles and submit these candidates to the next stages in the process of determining the registration. It can be appreciated by those practiced in the art that the foregoing was simply a known signal detection scheme, and that there are dozens of such schemes that can ultimately be created or borrowed. The simple requirement of the first stage process is to whittle down the candidate rotation angles to just a few, wherein more refined searches can then take over.

Fig. 34 essentially outlines the same type of gross searching in the power spectral domain. Here instead we first search for the gross scale of the concentric rings, stepping from a small scale through a large scale, rather than the rotation angle. The graph depicted in 1032 is the same normalized vector as in 1022 and 1024, but now the vector values are plotted as a function of angle around a semi-circle. The moving average denominator still needs to be calculated in the radial direction, rather than the tangential direction. As can be seen, a similar "peaking" in the normalized signal occurs when the scanned circle coincides with a graticule circle, giving rise to the plot 1040. The scale can then be found on the bottom plot by matching the known characteristics of the concentric rings (i.e. their radii) with the profile in 1040.

Fig. 35 depicts the second primary step in registering subliminal graticules of the type in Fig. 29. Once we have found a few rotation candidates from the methods of Fig. 33, we then

take the plots of the candidate angles of the type of 1022 and 1024 and perform what the inventor refers to as a "scaled kernel" matched filtering operation on those vectors. The scaled kernel refers to the fact that the kernel in this case is a known non-harmonic relationship of frequencies, represented as the lines with x's at the top in 1042 and 1044, and that the scale of these frequencies is swept through some pre-determined range, such as 25% to 400% of some expected scale at 100%. The matched filter operation simply adds the resultant multiplied values of the scaled frequencies and their plot counterparts. Those practiced in the art will recognize the similarity of this operation with the very well known matched filter operation. The resulting plot of the matched filter operation will look something like 1046 at the bottom of Fig. 35. Each candidate angle from the first step will generate its own such plot, and at this point the highest value of all of the plots will become our candidate scale, and the angle corresponding to the highest value will become our primary candidate rotation angle. Likewise for graticules of the type in Fig. 30, a similar "scaled-kernel" matched filtering operation is performed on the plot 1040 of Fig. 34. This generally provides for a single candidate scale factor. Then, using the stored phase plots 1012, 1014 and 1016 of Fig. 32, a more traditional matched filtering operation is applied between these stored plots (as kernels), and the measured phase profiles along the half-circles at the previously found scale.

The last step in registering graticules of the type in Fig. 29 is to perform a garden variety matched filter between the known (either spectral or spatial) profile of the graticule with the suspect image. Since both the rotation, scale and orientation are now known from previous steps, this matched filtering operation is straightforward. If the accuracies and precision of preceding steps have not exceeded design specifications in the process, then a simple micro-search can be performed in the small neighborhood about the two parameters scale and rotation, a matched filter operation performed, and the highest value found will determine a "fine tuned" scale and rotation. In this way, the scale and rotation can be found to within the degree set by the noise and cross-talk of the suspect image itself. Likewise, once the scale and rotation of the graticules of the type in Fig. 30 are found, then a straightforward matched filter operation can complete the registration process, and similar "fine tuning" can be applied.

Moving on to a variant of the use of the graticules of the type in Fig. 29, Fig. 36 presents the possibility for finding the subliminal graticules without the need for performing a

computationally expensive 2 dimensional FFT (fast fourier transform). In situations where computational overhead is a major issue, then the search problem can be reduced to a series of one-dimensional steps. Fig. 36 broadly depicts how to do this. The figure at the top left is an arbitrary image in which the graticules of the type of Fig. 29 have been embedded. Starting at angle 0, and finishing with an angle just below 180 degrees, and stepping by, for example 5 degrees, the grey values along the depicted columns can be simply added to create a resulting column-integrated scan, 1058. The figure in the top right, 1052, depicts one of the many angles at which this will be performed. This column-integrated scan then is transformed into its fourier representation using the less computationally expensive 1 dimensional FFT. This is then turned into a magnitude or "power" plot (the two are different), and a similar normalized vector version created just like 1022 and 1024 in Fig. 33. The difference now is that as the angle approaches the proper angles of the graticules, slowly the tell-tale peaks begin to appear in the 1024-like plots, but they generally show up at higher frequencies than expected for a given scale, since we are generally slightly off on our rotation. It remains to find the angle which maximizes the peak signals, thus zooming in on the proper rotation. Once the proper rotation is found, then the scaled kernel matched filter process can be applied, followed by traditional matched filtering, all as previously described. Again, the sole idea of the "short-cut" of Fig. 36 is to greatly reduce the computational overhead in using the graticules of the type in Fig. 29. The inventor has not reduced this method of Fig. 36 to practice and currently has no data on precisely how much computational savings, if any, will be realized. These efforts will be part of application specific development of the method.

Fig. 37 simply summarizes, in order of major process steps, the methods revolving around the graticules of the type in Fig. 29.

In another variant embodiment, the graticule energy is not concentrated around the 45 degree angles in the spatial frequency domain. (Some compression algorithms, such as JPEG, tend to particularly attenuate image energy at this orientation.) Instead, the energy is more widely spatially spread. Fig. 29A shows one such distribution. The frequencies near the axes, and near the origin are generally avoided, since this is where the image energy is most likely concentrated.

Detection of this energy in a suspect image again relies on techniques like that reviewed above. However, instead of first identifying the axes, then the rotation, and then the scale, a more global pattern matching procedure is performed in which all are determined in a brute force effort. Those skilled in the art will recognize that the Fourier-Mellin transform is well suited for use in such pattern matching problems.

The foregoing principles find application, for example, in photo-duplication kiosks. Such devices typically include a lens for imaging a customer-provided original (e.g. a photographic print or film) onto an opto-electronic detector, and a print-writing device for exposing and developing an emulsion substrate (again photographic paper or film) in accordance with the image data gathered by the detector. The details of such devices are well known to those skilled in the art, and are not belabored here.

In such systems, a memory stores data from the detector, and a processor (e.g. a Pentium microprocessor with associated support components) can be used to process the memory data to detect the presence of copyright data steganographically encoded therein. If such data is detected, the print-writing is interrupted.

To avoid defeat of the system by manual rotation of the original image off-axis, the processor desirably implements the above-described technique to effect automatic registration of the original, notwithstanding scale, rotation, and origin offset factors. If desired, a digital signal processing board can be employed to offload certain of the FFT processing from the main (e.g. Pentium) processor. After a rotated/scaled image is registered, detection of any steganographically encoded copyright notice is straightforward and assures the machine will not be used in violation of a photographer's copyright.

While the techniques disclosed above have make use of applicant's preferred steganographic encoding methods, the principles thereof are more widely applicable and can be used in many instances in which automatic registration of an image is to be effected.

USE OF EMBEDDED SIGNATURES IN VIDEO, WHEREIN A VIDEO DATA STREAM EFFECTIVELY SERVES AS A HIGH-SPEED ONE WAY MODEM

Through use of the universal coding system outlined in earlier sections, and through use of master snowy frames which change in a simple fashion frame to frame, a simple receiver can be designed such that it has pre-knowledge of the changes in the master snowy frames and can therefore read a changing N-bit message word frame by frame (or I-frame by I-frame as the case may be in MPEG video). In this way, a motion picture sequence can be used as a high speed one-way information channel, much like a one-way modem. Consider, for example, a frame of video data with N scan lines which is steganographically encoded to effect the transmission of an N-bit message. If there are 484 scan lines in a frame (N), and frames change 30 times a second, an information channel with a capacity comparable to a 14.4 kilobaud modem is achieved.

In actual practice, a data rate substantially in excess of N bits per frame can usually be achieved, yielding transmission rates nearer that of ISDN circuits.

FRAUD PREVENTION IN WIRELESS COMMUNICATIONS

In the cellular telephone industry, hundreds of millions of dollars of revenue is lost each year through theft of services. While some services are lost due to physical theft of cellular telephones, the more pernicious threat is posed by cellular telephone hackers.

Cellular telephone hackers employ various electronic devices to mimic the identification signals produced by an authorized cellular telephone. (These signals are sometimes called authorization signals, verification numbers, signature data, etc.) Often, the hacker learns of these signals by eavesdropping on authorized cellular telephone subscribers and recording the data exchanged with the cell cite. By artful use of this data, the hacker can impersonate an authorized subscriber and dupe the carrier into completing pirate calls.

In the prior art, identification signals are segregated from the voice signals. Most commonly, they are temporally separated, e.g. transmitted in a burst at the time of call origination. Voice data passes through the channel only after a verification operation has taken place on this identification data. (Identification data is also commonly included in data packets sent during the transmission.) Another approach is to spectrally separate the identification, e.g. in a spectral subband outside that allocated to the voice data.

Other fraud-deterrent schemes have also been employed. One class of techniques monitors characteristics of a cellular telephone's RF signal to identify the originating phone. Another class of techniques uses handshaking protocols, wherein some of the data returned by the cellular telephone is based on an algorithm (e.g. hashing) applied to random data sent thereto.

Combinations of the foregoing approaches are also sometimes employed.

U.S. Patents 5,465,387, 5,454,027, 5,420,910, 5,448,760, 5,335,278, 5,345,595, 5,144,649, 5,204,902, 5,153,919 and 5,388,212 detail various cellular telephone systems, and fraud deterrence techniques used therein. The disclosures of these patents are incorporated by reference.

As the sophistication of fraud deterrence systems increases, so does the sophistication of cellular telephone hackers. Ultimately, hackers have the upper hand since they recognize that all prior art systems are vulnerable to the same weakness: the identification is based on some attribute of the cellular telephone transmission outside the voice data. Since this attribute is segregated from the voice data, such systems will always be susceptible to pirates who electronically "patch" their voice into a composite electronic signal having the attribute(s) necessary to defeat the fraud deterrence system.

To overcome this failing, preferred embodiments of this aspect of the present technology steganographically encode the voice signal with identification data, resulting in "in-band" signalling (in-band both temporally and spectrally). This approach allows the carrier to monitor the user's voice signal and decode the identification data therefrom.

In one such form of the technology, some or all of the identification data used in the prior art (e.g. data transmitted at call origination) is repeatedly steganographically encoded in the user's voice signal as well. The carrier can thus periodically or aperiodically check the identification data accompanying the voice data with that sent at call origination to ensure they match. If they do not, the call is identified as being hacked and steps for remediation can be instigated such as interrupting the call.

In another form of the technology, a randomly selected one of several possible messages is repeatedly steganographically encoded on the subscriber's voice. An index sent to the cellular carrier at call set-up identifies which message to expect. If the message steganographically decoded by the cellular carrier from the subscriber's voice does not match that expected, the call is identified as fraudulent.

In a preferred form of this aspect of the technology, the steganographic encoding relies on a pseudo random data signal to transform the message or identification data into a low level noise-like signal superimposed on the subscriber's digitized voice signal. This pseudo random data signal is known, or knowable, to both the subscriber's telephone (for encoding) and to the cellular carrier (for decoding). Many such embodiments rely on a deterministic pseudo random number generator seeded with a datum known to both the telephone and the carrier. In simple embodiments this seed can remain constant from one call to the next (e.g. a telephone ID number). In more complex embodiments, a pseudo-one-time pad system may be used, wherein a new seed is used for each session (i.e. telephone call). In a hybrid system, the telephone and cellular carrier each have a reference noise key (e.g. 10,000 bits) from which the telephone selects a field of bits, such as 50 bits beginning at a randomly selected offset, and each uses this excerpt as the seed to generate the pseudo random data for encoding. Data sent from the telephone to the carrier (e.g. the offset) during call set-up allows the carrier to reconstruct the same pseudo random data for use in decoding. Yet further improvements can be derived by borrowing basic techniques from the art of cryptographic communications and applying them to the steganographically encoded signal detailed in this disclosure.

Details of applicant's preferred techniques for steganographic encoding/decoding with a pseudo random data stream are more particularly detailed in the previous portions of this specification, but the present technology is not limited to use with such techniques.

The reader is presumed to be familiar with cellular communications technologies. Accordingly, details known from prior art in this field aren't belabored herein.

Referring to Fig. 38, an illustrative cellular system includes a telephone 2010, a cell site 2012, and a central office 2014.

Conceptually, the telephone may be viewed as including a microphone 2016, an A/D converter 2018, a data formatter 2020, a modulator 2022, an RF section 2024, an antenna 2026, a demodulator 2028, a data unformatter 2030, a D/A converter 2032, and a speaker 2034.

In operation, a subscriber's voice is picked up by the microphone 2016 and converted to digital form by the A/D converter 2018. The data formatter 2020 puts the digitized voice into packet form, adding synchronization and control bits thereto. The modulator 2022 converts this digital data stream into an analog signal whose phase and/or amplitude properties change in accordance with the data being modulated. The RF section 2024 commonly translates this time-varying signal to one or more intermediate frequencies, and finally to a UHF transmission frequency. The RF section thereafter amplifies it and provides the resulting signal to the antenna 2026 for broadcast to the cell site 2012.

The process works in reverse when receiving. A broadcast from the cell cite is received through the antenna 2026. RF section 2024 amplifies and translates the received signal to a different frequency for demodulation. Demodulator 2028 processes the amplitude and/or phase variations of the signal provided by the RF section to produce a digital data stream corresponding thereto. The data unformatter 2030 segregates the voice data from the associated synchronization/control data, and passes the voice data to the D/A converter for conversion into analog form. The output from the D/A converter drives the speaker 2034, through which the subscriber hears the other party's voice.

The cell site 2012 receives broadcasts from a plurality of telephones 2010, and relays the data received to the central office 2014. Likewise, the cell site 2012 receives outgoing data from the central office and broadcasts same to the telephones.

The central office 2014 performs a variety of operations, including call authentication, switching, and cell hand-off.

(In some systems, the functional division between the cell site and the central station is different than that outlined above. Indeed, in some systems, all of this functionality is provided at a single site.)

In an exemplary embodiment of this aspect of the technology, each telephone 2010 additionally includes a steganographic encoder 2036. Likewise, each cell site 2012 includes a steganographic decoder 2038. The encoder operates to hide an auxiliary data signal among the signals representing the subscriber's voice. The decoder performs the reciprocal function, discerning the auxiliary data signal from the encoded voice signal. The auxiliary signal serves to verify the legitimacy of the call.

An exemplary steganographic encoder 2036 is shown in Fig. 39.

The illustrated encoder 2036 operates on digitized voice data, auxiliary data, and pseudo-random noise (PRN) data. The digitized voice data is applied at a port 2040 and is provided, e.g., from A/D converter 2018. The digitized voice may comprise 8-bit samples. The auxiliary data is applied at a port 2042 and comprises, in one form of the technology, a stream of binary data uniquely identifying the telephone 2010. (The auxiliary data may additionally include administrative data of the sort conventionally exchanged with a cell site at call set-up.) The pseudo-random noise data is applied at a port 2044 and can be, e.g., a signal that randomly alternates between "-1" and "1" values. (More and more cellular phones are incorporating spread spectrum capable circuitry, and this pseudo-random noise signal and other aspects of this technology can often "piggy-back" or share the circuitry which is already being applied in the basic operation of a cellular unit).

For expository convenience, it is assumed that all three data signals applied to the encoder 2036 are clocked at a common rate, although this is not necessary in practice.

In operation, the auxiliary data and PRN data streams are applied to the two inputs of a logic circuit 2046. The output of circuit 2046 switches between -1 and +1 in accordance with the following table:

AUX	PRN	OUTPUT
0	-1	1
0	1	-1
1	-1	-1
1	1	1

(If the auxiliary data signal is conceptualized as switching between -1 and 1, instead of 0 and 1, it will be seen that circuit 2046 operates as a one-bit multiplier.)

The output from gate 2046 is thus a bipolar data stream whose instantaneous value changes randomly in accordance with the corresponding values of the auxiliary data and the PRN data. It may be regarded as noise. However, it has the auxiliary data encoded therein. The auxiliary data can be extracted if the corresponding PRN data is known.

The noise-like signal from gate 2046 is applied to the input of a scaler circuit 2048. Scaler circuit scales (e.g. multiplies) this input signal by a factor set by a gain control circuit 2050. In the illustrated embodiment, this factor can range between 0 and 15. The output from scaler circuit 2048 can thus be represented as a five-bit data word (four bits, plus a sign bit) which changes each clock cycle, in accordance with the auxiliary and PRN data, and the scale

factor. The output from the scaler circuit may be regarded as "scaled noise data" (but again it is "noise" from which the auxiliary data can be recovered, given the PRN data).

The scaled noise data is summed with the digitized voice data by a summer 2051 to provide the encoded output signal (e.g. binarily added on a sample by sample basis). This output signal is a composite signal representing both the digitized voice data and the auxiliary data.

The gain control circuit 2050 controls the magnitude of the added scaled noise data so its addition to the digitized voice data does not noticeably degrade the voice data when converted to analog form and heard by a subscriber. The gain control circuit can operate in a variety of ways.

One is a logarithmic scaling function. Thus, for example, voice data samples having decimal values of 0, 1 or 2 may be correspond to scale factors of unity, or even zero, whereas voice data samples having values in excess of 200 may correspond to scale factors of 15. Generally speaking, the scale factors and the voice data values correspond by a square root relation. That is, a four-fold increase in a value of the voice data corresponds to approximately a two-fold increase in a value of the scaling factor associated therewith. Another scaling function would be linear as derived from the average power of the voice signal.

(The parenthetical reference to zero as a scaling factor alludes to cases, e.g., in which the digitized voice signal sample is essentially devoid of information content.)

More satisfactory than basing the instantaneous scaling factor on a single voice data sample, is to base the scaling factor on the dynamics of several samples. That is, a stream of digitized voice data which is changing rapidly can camouflage relatively more auxiliary data than a stream of digitized voice data which is changing slowly. Accordingly, the gain control circuit 2050 can be made responsive to the first, or preferably the second- or higher-order derivative of the voice data in setting the scaling factor.

In still other embodiments, the gain control block 2050 and scaler 2048 can be omitted entirely.

(Those skilled in the art will recognize the potential for "rail errors" in the foregoing systems. For example, if the digitized voice data consists of 8-bit samples, and the samples span the entire range from 0 to 255 (decimal), then the addition or subtraction of scaled noise to/from the input signal may produce output signals that cannot be represented by 8 bits (e.g. -2, or 257). A number of well-understood techniques exist to rectify this situation, some of them proactive and some of them reactive. Among these known techniques are: specifying that the digitized voice data shall not have samples in the range of 0-4 or 241-255, thereby safely permitting combination with the scaled noise signal; and including provision for detecting and adaptively modifying digitized voice samples that would otherwise cause rail errors.)

Returning to the telephone 2010, an encoder 2036 like that detailed above is desirably interposed between the A/D converter 2018 and the data formatter 2020, thereby serving to steganographically encode all voice transmissions with the auxiliary data. Moreover, the circuitry or software controlling operation of the telephone is arranged so that the auxiliary data is encoded repeatedly. That is, when all bits of the auxiliary data have been encoded, a pointer loops back and causes the auxiliary data to be applied to the encoder 2036 anew. (The auxiliary data may be stored at a known address in RAM memory for ease of reference.)

It will be recognized that the auxiliary data in the illustrated embodiment is transmitted at a rate one-eighth that of the voice data. That is, for every 8-bit sample of voice data, scaled noise data corresponding to a single bit of the auxiliary data is sent. Thus, if voice samples are sent at a rate of 4800 samples/second, auxiliary data can be sent at a rate of 4800 bits/second. If the auxiliary data is comprised of 8-bit symbols, auxiliary data can be conveyed at a rate of 600 symbols/second. If the auxiliary data consists of a string of even 60 symbols, each second of voice conveys the auxiliary data ten times. (Significantly higher auxiliary data rates can be achieved by resorting to more efficient coding techniques, such as limited-symbol codes (e.g. 5- or 6-bit codes), Huffman coding, etc.) This highly redundant transmission of the auxiliary data permits lower amplitude scaled noise data to be used while still providing sufficient signal-to-noise headroom to assure reliable decoding -- even in the relatively noisy environment associated with radio transmissions.

Turning now to Fig. 40, each cell site 2012 has a steganographic decoder 2038 by which it can analyze the composite data signal broadcast by the telephone 2010 to discern and separate the auxiliary data and digitized voice data therefrom. (The decoder desirably works on unformatted data (i.e. data with the packet overhead, control and administrative bits removed; this is not shown for clarity of illustration).

The decoding of an unknown embedded signal (i.e. the encoded auxiliary signal) from an unknown voice signal is best done by some form of statistical analysis of the composite data signal. The techniques therefor discussed above are equally applicable here. For example, the entropy-based approach can be utilized. In this case, the auxiliary data repeats every 480 bits (instead of every 8). As above, the entropy-based decoding process treats every 480th sample of the composite signal in like fashion. In particular, the process begins by adding to the 1st, 481st, 861st, etc. samples of the composite data signal the PRN data with which these samples were encoded. (That is, a set of sparse PRN data is added: the original PRN set, with all but every 480th datum zeroed out.) The localized entropy of the resulting signal around these points (i.e. the composite data signal with every 480th sample modified) is then computed.

The foregoing step is then repeated, this time subtracting the PRN data corresponding thereto from the 1st, 481st, 961st, etc. composite data samples.

One of these two operations will counteract (e.g. undo) the encoding process and reduce the resulting signal's entropy; the other will aggravate it. If adding the sparse PRN data to the composite data reduces its entropy, then this data must earlier have been subtracted from the original voice signal. This indicates that the corresponding bit of the auxiliary data signal was a "0" when these samples were encoded. (A "0" at the auxiliary data input of logic circuit 46 caused it to produce an inverted version of the corresponding PRN datum as its output datum, resulting in subtraction of the corresponding PRN datum from the voice signal.)

Conversely, if subtracting the sparse PRN data from the composite data reduces its entropy, then the encoding process must have earlier added this noise. This indicates that the value of the auxiliary data bit was a "1" when samples 1, 481, 961, etc., were encoded.

By noting in which case entropy is lower by (a) adding or (b) subtracting a sparse set of PRN data to/from the composite data, it can be determined whether the first bit of the auxiliary data is (a) a "0", or (b) a "1." (In real life applications, in the presence of various distorting phenomena, the composite signal may be sufficiently corrupted so that neither adding nor subtracting the sparse PRN data actually reduces entropy. Instead, both operations will increase entropy. In this case, the "correct" operation can be discerned by observing which operation increases the entropy less.)

The foregoing operations can then be conducted for the group of spaced samples of the composite data beginning with the second sample (i.e. 2, 482, 962, ...). The entropy of the resulting signals indicate whether the second bit of the auxiliary data signal is a "0" or a "1." Likewise with the following 478 groups of spaced samples in the composite signal, until all 480 bits of the code word have been discerned.

As discussed above, correlation between the composite data signal and the PRN data can also be used as a statistical detection technique. Such operations are facilitated in the present context since the auxiliary data whose encoded representation is sought, is known, at least in large part, a priori. (In one form of the technology, the auxiliary data is based on the authentication data exchanged at call set-up, which the cellular system has already received and logged; in another form (detailed below), the auxiliary data comprises a predetermined message.) Thus, the problem can be reduced to determining whether an expected signal is present or not (rather than looking for an entirely unknown signal). Moreover, data formatter 2020 breaks the composite data into frames of known length. (In a known GSM implementation, voice data is sent in time slots which convey 114 data bits each.) By padding the auxiliary data as necessary, each repetition of the auxiliary data can be made to start, e.g., at the beginning of such a frame of data. This, too, simplifies the correlation determinations, since 113 of every 114 possible bit alignments can be ignored (facilitating decoding even if none of the auxiliary data is known a priori).

Again, this wireless fraud detection poses the now-familiar problem of detecting known signals in noise, and the approaches discussed earlier are equally applicable here.

Where, as here, the location of the auxiliary signal is known a priori (or more accurately, known to fall within one of a few discrete locations, as discussed above), then the matched filter approach can often be reduced to a simple vector dot product between a set of sparse PRN data, and mean-removed excerpts of the composite signal corresponding thereto. (Note that the PRN data need not be sparse and may arrive in contiguous bursts, such as in British patent publication 2,196,167 mentioned earlier wherein a given bit in a message has contiguous PRN values associated with it.) Such a process steps through all 480 sparse sets of PRN data and performs corresponding dot product operations. If the dot product is positive, the corresponding bit of the auxiliary data signal is a "1;" if the dot product is negative, the corresponding bit of the auxiliary data signal is a "0." If several alignments of the auxiliary data signal within the framed composite signal are possible, this procedure is repeated at each candidate alignment, and the one yielding the highest correlation is taken as true. (Once the correct alignment is determined for a single bit of the auxiliary data signal, the alignment of all the other bits can be determined therefrom. "Alignment," perhaps better known as "synchronization," can be achieved by primarily through the very same mechanisms which lock on and track the voice signal itself and allow for the basic functioning of the cellular unit).

Security Considerations

Security of the presently described embodiments depends, in large part, on security of the PRN data and/or security of the auxiliary data. In the following discussion, a few of many possible techniques for assuring the security of these data are discussed.

In a first embodiment, each telephone 2010 is provided with a long noise key unique to the telephone. This key may be, e.g., a highly unique 10,000 bit string stored in ROM. (In most applications, keys substantially shorter than this may be used.)

The central office 2014 has access to a secure disk 2052 on which such key data for all authorized telephones are stored. (The disk may be remote from the office itself.)

Each time the telephone is used, fifty bits from this noise key are identified and used as the seed for a deterministic pseudo random number generator. The data generated by this PRN generator serve as the PRN data for that telephone call.

The fifty bit seed can be determined, e.g., by using a random number generator in the telephone to generate an offset address between 0 and 9,950 each time the telephone is used to place a call. The fifty bits in the noise key beginning at this offset address are used as the seed.

During call setup, this offset address is transmitted by the telephone, through the cell site 2012, to the central office 2014. There, a computer at the central office uses the offset address to index its copy of the noise key for that telephone. The central office thereby identifies the same 50 bit seed as was identified at the telephone. The central office 2014 then relays these 50 bits to the cell site 2012, where a deterministic noise generator like that in the telephone generates a PRN sequence corresponding to the 50 bit key and applies same to its decoder 2038.

By the foregoing process, the same sequence of PRN data is generated both at the telephone and at the cell site. Accordingly, the auxiliary data encoded on the voice data by the telephone can be securely transmitted to, and accurately decoded by, the cell site. If this auxiliary data does not match the expected auxiliary data (e.g. data transmitted at call set-up), the call is flagged as fraudulent and appropriate remedial action is taken.

It will be recognized that an eavesdropper listening to radio transmission of call set-up information can intercept only the randomly generated offset address transmitted by the telephone to the cell site. This data, alone, is useless in pirating calls. Even if the hacker had access to the signals provided from the central office to the cell site, this data too is essentially useless: all that is provided is a 50 bit seed. Since this seed is different for nearly each call (repeating only 1 out of every 9,950 calls), it too is unavailing to the hacker.

In a related system, the entire 10,000 bit noise key can be used as a seed. An offset address randomly generated by the telephone during call set-up can be used to identify where, in the PRN data resulting from that seed, the PRN data to be used for that session is to begin.

(Assuming 4800 voice samples per second, 4800 PRN data are required per second, or about 17 million PRN data per hour. Accordingly, the offset address in this variant embodiment will likely be far larger than the offset address described above.)

In this variant embodiment, the PRN data used for decoding is preferably generated at the central station from the 10,000 bit seed, and relayed to the cell site. (For security reasons, the 10,000 bit noise key should not leave the security of the central office.)

In variants of the foregoing systems, the offset address can be generated by the central station or at the cell site, and relayed to the telephone during call set-up, rather than vice versa.

In another embodiment, the telephone 2010 may be provided with a list of one-time seeds, matching a list of seeds stored on the secure disk 2052 at the central office. Each time the telephone is used to originate a new call, the next seed in the list is used. By this arrangement, no data needs to be exchanged relating to the seed; the telephone and the carrier each independently know which seed to use to generate the pseudo random data sequence for the current session.

In such an embodiment, the carrier can determine when the telephone has nearly exhausted its list of seeds, and can transmit a substitute list (e.g. as part of administrative data occasionally provided to the telephone). To enhance security, the carrier may require that the telephone be returned for manual reprogramming, to avoid radio transmission of this sensitive information. Alternatively, the substitute seed list can be encrypted for radio transmission using any of a variety of well known techniques.

In a second class of embodiments, security derives not from the security of the PRN data, but from security of the auxiliary message data encoded thereby. One such system relies on transmission of a randomly selected one of 256 possible messages.

In this embodiment, a ROM in the telephone stores 256 different messages (each message may be, e.g., 128 bits in length). When the telephone is operated to initiate a call, the telephone

randomly generates a number between 1 and 256, which serves as an index to these stored messages. This index is transmitted to the cell site during call set-up, allowing the central station to identify the expected message from a matching database on secure disk 2052 containing the same 256 messages. (Each telephone has a different collection of messages.) (Alternatively, the carrier may randomly select the index number during call set-up and transmit it to the telephone, identifying the message to be used during that session.) In a theoretically pure world where proposed attacks to a secure system are only mathematical in nature, much of these additional layers of security might seem superfluous. (The addition of these extra layers of security, such as differing the messages themselves, simply acknowledge that the designer of actual public-functioning secure systems will face certain implementation economics which might compromise the mathematical security of the core principles of this technology, and thus these auxiliary layers of security may afford new tools against the inevitable attacks on implementation).

Thereafter, all voice data transmitted by the telephone for the duration of that call is steganographically encoded with the indexed message. The cell site checks the data received from the telephone for the presence of the expected message. If the message is absent, or if a different message is decoded instead, the call is flagged as fraudulent and remedial action is taken.

In this second embodiment, the PRN data used for encoding and decoding can be as simple or complex as desired. A simple system may use the same PRN data for each call. Such data may be generated, e.g., by a deterministic PRN generator seeded with fixed data unique to the telephone and known also by the central station (e.g. a telephone identifier), or a universal noise sequence can be used (i.e. the same noise sequence can be used for all telephones). Or the pseudo random data can be generated by a deterministic PRN generator seeded with data that changes from call to call (e.g. based on data transmitted during call set-up identifying, e.g., the destination telephone number, etc.). Some embodiments may seed the pseudo random number generator with data from a preceding call (since this data is necessarily known to the telephone and the carrier, but is likely not known to pirates).

Naturally, elements from the foregoing two approaches can be combined in various ways, and supplemented by other features. The foregoing embodiments are exemplary only, and do not

begin to catalog the myriad approaches which may be used. Generally speaking, any data which is necessarily known or knowable by both the telephone and the cell site/central station, can be used as the basis for either the auxiliary message data, or the PRN data by which it is encoded.

Since the preferred embodiments of this aspect of the present technology each redundantly encodes the auxiliary data throughout the duration of the subscriber's digitized voice, the auxiliary data can be decoded from any brief sample of received audio. In the preferred forms of this aspect of the technology, the carrier repeatedly checks the steganographically encoded auxiliary data (e.g. every 10 seconds, or at random intervals) to assure that it continues to have the expected attributes.

While the foregoing discussion has focused on steganographically encoding a transmission from a cellular telephone, it will be recognized that transmissions to a cellular telephone can be steganographically encoded as well. Such arrangements find applicability, e.g., in conveying administrative data (i.e. non-voice data) from the carrier to individual telephones. This administrative data can be used, for example, to reprogram parameters of targeted cellular telephones (or all cellular telephones) from a central location, to update seed lists (for systems employing the above-described on-time pad system), to apprise "roaming" cellular telephones of data unique to an unfamiliar local area, etc.

In some embodiments, the carrier may steganographically transmit to the cellular telephone a seed which the cellular phone is to use in its transmissions to the carrier during the remainder of that session.

While the foregoing discussion has focused on steganographic encoding of the baseband digitized voice data, artisans will recognize that intermediate frequency signals (whether analog or digital) can likewise be steganographically encoded in accordance with principles of the technology. An advantage of post-baseband encoding is that the bandwidth of these intermediate signals is relatively large compared with the baseband signal, allowing more auxiliary data to be encoded therein, or allowing a fixed amount of auxiliary data to be repeated more frequently during transmission. (If steganographic encoding of an intermediate signal is employed, care

should be taken that the perturbations introduced by the encoding are not so large as to interfere with reliable transmission of the administrative data, taking into account any error correcting facilities supported by the packet format).

Those skilled in the art will recognize that the auxiliary data, itself, can be arranged in known ways to support error detecting, or error correcting capabilities by the decoder 38. The interested reader is referred, e.g., to Rorabaugh, *Error Coding Cookbook*, McGraw Hill, 1996, one of many readily available texts detailing such techniques.

While the preferred embodiment of this aspect of the technology is illustrated in the context of a cellular system utilizing packetized data, other wireless systems do not employ such conveniently framed data. In systems in which framing is not available as an aid to synchronization, synchronization marking can be achieved within the composite data signal by techniques such as that detailed in applicant's prior applications. In one class of such techniques, the auxiliary data itself has characteristics facilitating its synchronization. In another class of techniques, the auxiliary data modulates one or more embedded carrier patterns which are designed to facilitate alignment and detection.

As noted earlier, the principles of the technology are not restricted to use with the particular forms of steganographic encoding detailed above. Indeed, any steganographic encoding technique previously known, or hereafter invented, can be used in the fashion detailed above to enhance the security or functionality of cellular (or other wireless, e.g. PCS) communications systems. Likewise, these principles are not restricted to wireless telephones; any wireless transmission may be provided with an "in-band" channel of this type.

It will be recognized that systems for implementing applicant's technology can comprises dedicated hardware circuit elements, but more commonly comprise suitably programmed microprocessors with associated RAM and ROM memory (e.g. one such system in each of the telephone 2010, cell-site 2012, and central office 2014).

ENCODING BY BIT CELLS

The foregoing discussions have focused on incrementing or decrementing the values of individual pixels, or of groups of pixels (bumps), to reflect encoding of an auxiliary data signal combined with a pseudo random noise signal. The following discussion details a variant embodiment wherein the auxiliary data -- without pseudo randomization -- is encoded by patterned groups of pixels, here termed bit cells.

Referring to Figs 41A and 41B, two illustrative 2x2 bit cells are shown. Fig. 41A is used to represent a "0" bit of the auxiliary data, while Fig. 41B is used to represent a "1" bit. In operation, the pixels of the underlying image are tweaked up or down in accordance with the +/- values of the bit cells to represent one of these two bit values. (The magnitude of the tweaking at any given pixel, bit cell or region of the image can be a function of many factors, as detailed below. It is the sign of the tweaking that defines the characteristic pattern.) In decoding, the relative biases of the encoded pixels are examined (using techniques described above) to identify, for each corresponding region of the encoded image, which of the two patterns is represented.

While the auxiliary data is not explicitly randomized in this embodiment, it will be recognized that the bit cell patterns may be viewed as a "designed" carrier signal, as discussed above.

The substitution of the previous embodiments' pseudo random noise with the present "designed" information carrier affords an advantage: the bit cell patterning manifests itself in Fourier space. Thus, the bit cell patterning can act like the subliminal digital graticules discussed above to help register a suspect image to remove scale/rotation errors. By changing the size of the bit cell, and the pattern therein, the location of the energy thereby produced in the spatial transform domain can be tailored to optimize independence from typical imagery energy and facilitate detection.

(While the foregoing discussion contemplates that the auxiliary data is encoded directly -- without randomization by a PRN signal, in other embodiments, randomization can of course be used.)

MORE ON PERCEPTUALLY ADAPTIVE SIGNING

In several of the above-detailed embodiments, the magnitude of the signature energy was tailored on a region-by-region basis to reduce its visibility in an image (or its audibility in a sound, etc.). In the following discussion, applicant more particularly considers the issue of hiding signature energy in an image, the separate issues thereby posed, and solutions to each of these issues.

The goal of the signing process, beyond simply functioning, is to maximize the "numeric detectability" of an embedded signature while meeting some form of fixed "visibility/acceptability threshold" set by a given user/creator.

In service to design toward this goal, imagine the following three axis parameter space, where two of the axes are only half-axes (positive only), and the third is a full axis (both negative and positive). This set of axes define two of the usual eight octal spaces of euclidean 3-space. As things refine and "deservedly separable" parameters show up on the scene (such as "extended local visibility metrics"), then they can define their own (generally) half-axis and extend the following example beyond three dimensions.

The signing design goal becomes optimally assigning a "gain" to a local bump based on its coordinates in the above defined space, whilst keeping in mind the basic needs of doing the operations fast in real applications. To begin with, the three axes are the following. We'll call the two half axes x and y, while the full axis will be z.

The x axis represents the luminance of the singular bump. The basic idea is that you can squeeze a little more energy into bright regions as opposed to dim ones. It is important to note that when true "psycho-linear - device independent" luminance values (pixel DN's) come along, this axis might become superfluous, unless of course if the luminance value couples into the other operative axes (e.g. C*xy). For now, this is here as much due to the sub-optimality of current quasi-linear luminance coding.

The y axis is the "local hiding potential" of the neighborhood within which the bump finds itself. The basic idea is that flat regions have a low hiding potential since the eye can detect subtle changes in such regions, whereas complex textured regions have a high hiding potential. Long lines and long edges tend toward the lower hiding potential since "breaks and choppiness" in nice smooth long lines are also somewhat visible, while shorter lines and edges, and mosaics thereof, tend toward the higher hiding potential. These latter notions of long and short are directly connected to processing time issues, as well to issues of the engineering resources needed to carefully quantify such parameters. Developing the working model of the y-axis will inevitably entail one part theory to one part picky-artist-empiricism. As the parts of the hodge-podge y-axis become better known, they can splinter off into their own independent axes if it's worth it.

The z-axis is the "with or against the grain" (discussed below) axis which is the full axis - as opposed to the other two half-axes. The basic idea is that a given input bump has a pre-existing bias relative to whether one wishes to encode a '1' or a '0' at its location, which to some non-trivial extent is a function of the reading algorithms which will be employed, whose (bias) magnitude is semi-correlated to the "hiding potential" of the y-axis, and, fortunately, can be used advantageously as a variable in determining what magnitude of a tweak value is assigned to the bump in question. The concomitant basic idea is that when a bump is already your friend (i.e. its bias relative to its neighbors already tends towards the desired delta value), then don't change it much. Its natural state already provides the delta energy needed for decoding, without altering the localized image value much, if at all. Conversely, if a bump is initially your enemy (i.e. its bias relative to its neighbors tends away from the delta sought to be imposed by the encoding), then change it an exaggerated amount. This later operation tends to reduce the excursion of this point relative to its neighbors, making the point less visibly conspicuous (a

highly localized blurring operation), while providing additional energy detectable when decoding. These two cases are termed "with the grain" and "against the grain" herein.

The above general description of the problem should suffice for many years. Clearly adding in chrominance issues will expand the definitions a bit, leading to a bit more signature bang for the visibility, and human visibility research which is applied to the problem of compression can equally be applied to this area but for diametrically opposed reasons. Here are guiding principles which can be employed in an exemplary application.

For speed's sake, local hiding potential can be calculated only based on a 3 by 3 neighborhood of pixels, the center one being signed and its eight neighbors. Beyond speed issues, there is also no data or coherent theory to support anything larger as well. The design issue boils down to canning the y-axis visibility thing, how to couple the luminance into this, and a little bit on the friend/enemy asymmetry thing. A guiding principle is to simply make a flat region zero, a classic pure maxima or minima region a "1.0" or the highest value, and to have "local lines", "smooth slopes", "saddle points" and whatnot fall out somewhere in between.

The exemplary application uses six basic parameters: 1) luminance; 2) difference from local average; 3) the asymmetry factor (with or against the grain); 4) minimum linear factor (our crude attempt at flat v. lines v. maxima); 5) bit plane bias factor; and 6) global gain (the user's single top level gain knob).

The Luminance, and Difference from Local Average parameters are straight forward, and their use is addressed elsewhere in this specification.

The Asymmetry factor is a single scalar applied to the "against the grain" side of the difference axis of number 2 directly above.

The Minimum Linear factor is admittedly crude but it should be of some service even in a 3 by 3 neighborhood setting. The idea is that true 2D local minima and maxima will be highly perturbed along each of the four lines travelling through the center pixel of the 3 by 3

neighborhood, while a visual line or edge will tend to flatten out at least one of the four linear profiles. [The four linear profiles are each 3 pixels in length, i.e., the top left pixel - center - bottom right; the top center - center - bottom center; the top right - center - bottom left; the right center - center - left center;]. Let's choose some metric of entropy as applied to three pixels in a row, perform this on all four linear profiles, then choose the minimum value for our ultimate parameter to be used as our 'y-axis.'

The Bit Plane Bias factor is an interesting creature with two faces, the pre-emptive face and the post-emptive face. In the former, you simply "read" the unsigned image and see where all the biases fall out for all the bit planes, then simply boost the "global gain" of the bit planes which are, in total, going against your desired message, and leave the others alone or even slightly lower their gain. In the post-emptive case, you churn out the whole signing process replete with the pre-emptive bit plane bias and the other 5 parameters listed here, and then you, e.g., run the signed image through heavy JPEG compression AND model the "gestalt distortion" of line screen printing and subsequent scanning of the image, and then you read the image and find out which bit planes are struggling or even in error, you appropriately beef up the bit plane bias, and you run through the process again. If you have good data driving the beefing process you should only need to perform this step once, or, you can easily Van-Cittertize the process (arcane reference to reiterate the process with some damping factor applied to the tweaks).

Finally, there is the Global Gain. The goal is to make this single variable the top level "intensity knob" (more typically a slider or other control on a graphical user interface) that the slightly curious user can adjust if they want to. The very curious user can navigate down advanced menus to get their experimental hands on the other five variables here, as well as others.

Visible Watermark

In certain applications it is desirable to apply a visible indicia to an image to indicate that it includes steganographically encoded data. In one embodiment, this indicia can be a lightly visible logo (sometimes termed a "watermark") applied to one corner of the image. This indicates that the image is a "smart" image, conveying data in addition to the imagery. A lightbulb is one suitable logo.

If marking of images becomes widespread (e.g., by software compatible with Adobe's image processing software), a user of such software can decode the embedded data from an image and consult a public registry to identify the proprietor of the image. In some embodiments, the registry can serve as the conduit through which appropriate royalty payments are forwarded to the proprietor for the user's use of an image. (In an illustrative embodiment, the registry is a server on the Internet, accessible via the World Wide Web, coupled to a database. The database includes detailed information on catalogued images (e.g. name, address, phone number of

proprietor, and a schedule of charges for different types of uses to which the image may be put), indexed by identification codes with which the images themselves are encoded. A person who decodes an image queries the registry with the codes thereby gleaned to obtain the desired data and, if appropriate, to forward electronic payment of a copyright royalty to the image's proprietor.)

Particular Data Formats

While the foregoing steganography techniques are broadly applicable, their commercial acceptance will be aided by establishment of standards setting forth which pixels/bit cells represent what. The following discussion proposes one set of possible standards. For expository convenience, this discussion focuses on decoding of the data; encoding follows in a straightforward manner.

Referring to Fig. 42, an image 1202 includes a plurality of tiled "signature blocks" 1204. (Partial signature blocks may be present at the image edges.) Each signature block 1204 includes an 8 x 8 array of sub-blocks 1206. Each sub-block 1206 includes an 8 x 8 array of bit cells 1208. Each bit cell comprises a 2 x 2 array of "bumps" 1210. Each bump 1210, in turn, comprises a square grouping of 16 individual pixels 1212.

The individual pixels 1212 are the smallest quanta of image data. In this arrangement, however, pixel values are not, individually, the data carrying elements. Instead, this role is served by bit cells 1208 (i.e. 2 x 2 arrays of bumps 1210). In particular, the bumps comprising the bits cells are encoded to assume one of the two patterns shown in Fig. 41. As noted earlier, the pattern shown in Fig. 41A represents a "0" bit, while the pattern shown in Fig. 41B represents a "1" bit. Each bit cell 1208 (64 image pixels) thus represents a single bit of the embedded data. Each sub-block 1206 includes 64 bit cells, and thus conveys 64 bits of embedded data.

(The nature of the image changes effected by the encoding follows the techniques set forth above under the heading MORE ON PERCEPTUALLY ADAPTIVE SIGNING; that discussion is not repeated here.)

In the illustrated embodiment, the embedded data includes two parts: control bits and message bits. The 16 bit cells 1208A in the center of each sub-block 1206 serve to convey 16 control bits. The surrounding 48 bit cells 1208B serve to convey 48 message bits. This 64-bit chunk of data is encoded in each of the sub-blocks 1206, and is repeated 64 times in each signature block 1204.

A digression: in addition to encoding of the image to redundantly embed the 64 control/message bits therein, the values of individual pixels are additionally adjusted to effect encoding of subliminal graticules through the image. In this embodiment, the graticules discussed in conjunction with Fig. 29A are used, resulting in an imperceptible texturing of the image. When the image is to be decoded, the image is transformed into the spatial domain, the Fourier-Mellin technique is applied to match the graticule energy points with their expected positions, and the processed data is then inverse-transformed, providing a registered image ready for decoding. (The sequence of first tweaking the image to effect encoding of the subliminal graticules, or first tweaking the image to effect encoding of the embedded data, is not believed to be critical. As presently practiced, the local gain factors (discussed above) are computed; then the data is encoded; then the subliminal graticule encoding is performed. (Both of these encoding steps make use of the local gain factors.))

Returning to the data format, once the encoded image has been thus registered, the locations of the control bits in sub-block 1206 are known. The image is then analyzed, in the aggregate (i.e. considering the "northwestern-most" sub-block 1206 from each signature block 1204), to determine the value of control bit #1 (represented in sub-block 1206 by bit cell 1208Aa). If this value is determined (e.g. by statistical techniques of the sort detailed above) to be a "1," this indicates that the format of the embedded data conforms to the standard detailed herein (the Digimarc Beta Data Format). According to this standard, control bit #2 (represented by bit cells 1208Ab) is a flag indicating whether the image is copyrighted. Control bit #3

(represented by bit cells 1208Ac) is a flag indicating whether the image is unsuitable for viewing by children. Certain of the remaining bits are used for error detection/correction purposes.

The 48 message bits of each sub block 1206 can be put to any use; they are not specified in this format. One possible use is to define a numeric "owner" field and a numeric "image/item" field (e.g. 24 bits each).

If this data format is used, each sub-block 1206 contains the entire control/message data, so same is repeated 64 times within each signature block of the image.

If control bit #1 is not a "1," then the format of the embedded data does not conform to the above described standard. In this case, the reading software analyzes the image data to determine the value of control bit #4. If this bit is set (i.e. equal to "1"), this signifies an embedded ASCII message. The reading software then examines control bits #5 and #6 to determine the length of the embedded ASCII message.

If control bits #5 and #6 both are "0," this indicates the ASCII message is 6 characters in length. In this case, the 48 bit cells 1208B surrounding the control bits 1208A are interpreted as six ASCII characters (8 bits each). Again, each sub-block 1206 contains the entire control/message data, so same is repeated 64 times within each signature block 1204 of the image.

If control bit #5 is "0" and control bit #6 is "1," this indicates the embedded ASCII message is 14 characters in length. In this case, the 48 bit cells 1208B surrounding the control bits 1208A are interpreted as the first six ASCII characters. The 64 bit cells 1208 of the immediately-adjoining sub-block 1220 are interpreted as the final eight ASCII characters.

Note that in this arrangement, the bit-cells 1208 in the center of sub-block 1220 are not interpreted as control bits. Instead, the entire sub-block serves to convey additional message bits. In this case there is just one group of control bits for two sub-blocks.

Also note than in this arrangement, pairs of sub-blocks 1206 contains the entire control/message data. so same is repeated 32 times within each signature block 1204 of the image.

Likewise if control bit #5 is "1" and control bit #6 is "0." This indicates the embedded ASCII message is 30 characters in length. In this case, 2 x 2 arrays of sub-blocks are used for each representation of the data. The 48 bit cells 1208B surrounding control bits 1208A are interpreted as the first six ASCII characters. The 64 bit cells of each of adjoining block 1220 are interpreted as representing the next 8 additional characters. The 64 bits cells of sub-block 1222 are interpreted as representing the next 8 characters. And the 64 bit cells of sub-block 1224 are interpreted as representing the final 8 characters. In this case, there is just one group of control bits for four sub-blocks. And the control/message data is repeated 16 times within each signature block 1204 of the image.

If control bits #5 and #6 are both "1"s, this indicates an ASCII message of programmable length. In this case, the reading software examines the first 16 bit cells 1208B surrounding the control bits. Instead of interpreting these bit cells as message bits, they are interpreted as additional control bits (the opposite of the case described above, where bit cells normally used to represent control bits represented message bits instead). In particular, the reading software interprets these 16 bits as representing, in binary, the length of the ASCII message. An algorithm is then applied to this data (matching a similar algorithm used during the encoding process) to establish a corresponding tiling pattern (i.e. to specify which sub-blocks convey which bits of the ASCII message, and which convey control bits.)

In this programmable-length ASCII message case, control bits are desirably repeated several times within a single representation of the message so that, e.g., there is one set of control bits for approximately every 24 ASCII characters. To increase packing efficiency, the tiling algorithm can allocate (divide) a sub-block so that some of its bit-cells are used for a first representation of the message, and others are used for another representation of the message.

Reference was earlier made to beginning the decoding of the registered image by considering the "northwestern-most" sub-block 1206 in each signature block 1204. This bears elaboration.

Depending on the data format used, some of the sub-blocks 1206 in each signature block 1204 may not include control bits. Accordingly, the decoding software desirably determines the data format by first examining the "northwestern-most" sub-block 1206 in each signature block 1204; the 16 bits cells in the centers of these sub-blocks will reliably represent control bits. Based on the value(s) of one or more of these bits (e.g. the Digimarc Beta Data Format bit), the decoding software can identify all other locations throughout each signature block 1204 where the control bits are also encoded (e.g. at the center of each of the 64 sub-blocks 1206 comprising a signature block 1204), and can use the larger statistical base of data thereby provided to extract the remaining control bits from the image (and to confirm, if desired, the earlier control bit(s) determination). After all control bits have thereby been discerned, the decoding software determines (from the control bits) the mapping of message bits to bit cells throughout the image.

To reduce the likelihood of visual artifacts, the numbering of bit cells within sub-blocks is alternated in a checkerboard-like fashion. That is, the "northwestern-most" bit cell in the "northwestern-most" sub-block is numbered "0." Numbering increases left to right, and successively through the rows, up to bit cell 63. Each sub-block diametrically adjoining one of its corners (i.e. sub-block 1224) has the same ordering of bit cells. But sub-blocks adjoining its edges (i.e. sub-blocks 1220 and 1222) have the opposite numbering. That is, the "northwestern-most" bit cell in sub-blocks 1220 and 1222 is numbered "63." Numbering decreases left to right, and successively through the rows, down to 0. Likewise throughout each signature block 1204.

In a variant of the Digimarc beta format, a pair of sub-blocks is used for each representation of the data, providing 128 bit cells. The center 16 bit cells 1208 in the first sub-block 1206 are used to represent control bits. The 48 remaining bit cells in that sub-block, together with all 64 bit cells 1208 in the adjoining sub-block 1220, are used to provide a 112-bit message field. Likewise for every pair of sub-blocks throughout each signature block 1204. In such an arrangement, each signature block 1204 thus includes 32 complete representations of the

encoded data (as opposed to 64 representations in the earlier-described standard). This additional length allows encoding of longer data strings, such as a numeric IP address (e.g. URL).

Obviously, numerous alternative data formats can be designed. The particular format used can be indicated to the decoding software by values of one or more control bits in the encoded image.

Other Applications

Before concluding, it may be instructive to review some of the other fields where principles of applicant's technology can be employed.

One is smart business cards, wherein a business card is provided with a photograph having unobtrusive, machine-readable contact data embedded therein. (The same function can be achieved by changing the surface microtopology of the card to embed the data therein.)

Another promising application is in content regulation. Television signals, images on the internet, and other content sources (audio, image, video, etc.) can have data indicating their "appropriateness" (i.e. their rating for sex, violence, suitability for children, etc.) actually embedded in the content itself rather than externally associated therewith. Television receivers, internet surfing software, etc., can discern such appropriateness ratings (e.g. by use of universal

code decoding) and can take appropriate action (e.g. not permitting viewing of an image or video, or play-back of an audio source).

In a simple embodiment of the foregoing, the embedded data can have one or more "flag" bits, as discussed earlier. One flag bit can signify "inappropriate for children." (Others can be. e.g., "this image is copyrighted" or "this image is in the public domain.") Such flag bits can be in a field of control bits distinct from an embedded message, or can -- themselves -- be the message. By examining the state of these flag bits, the decoder software can quickly apprise the user of various attributes of the image.

(As discussed earlier, control bits can be encoded in known locations in the image -- known relative to the subliminal graticules -- and can indicate the format of the embedded data (e.g. its length, its type, etc.) As such, these control bits are analogous to data sometimes conveyed in prior art file headers, but in this case they are embedded within an image, instead of prepended to a file.)

The field of merchandise marking is generally well served by familiar bar codes and universal product codes. However, in certain applications, such bar codes are undesirable (e.g. for aesthetic considerations, or where security is a concern). In such applications, applicant's technology may be used to mark merchandise, either through in innocuous carrier (e.g. a photograph associated with the product), or by encoding the microtopology of the merchandise's surface, or a label thereon.

There are applications -- too numerous to detail -- in which steganography can advantageously be combined with encryption and/or digital signature technology to provide enhanced security.

Medical records appear to be an area in which authentication is important. Steganographic principles -- applied either to film-based records or to the microtopology of documents -- can be employed to provide some protection against tampering.

Many industries, e.g. automobile and airline, rely on tags to mark critical parts. Such tags, however, are easily removed, and can often be counterfeited. In applications wherein better security is desired, industrial parts can be steganographically marked to provide an inconspicuous identification/authentication tag.

In various of the applications reviewed in this specification, different messages can be steganographically conveyed by different regions of an image (e.g. different regions of an image can provide different internet URLs, or different regions of a photocollage can identify different photographers). Likewise with other media (e.g. sound).

Some software visionaries look to the day when data blobs will roam the datawaves and interact with other data blobs. In such an era, it will be necessary for such blobs to have robust and incorruptible ways of identifying themselves. Steganographic techniques again hold much promise here.

Finally, message changing codes -- recursive systems in which steganographically encoded messages actually change underlying steganographic code patterns -- offer new levels of sophistication and security. Such message changing codes are particularly well suited to applications such as plastic cash cards where time-changing elements are important to enhance security.

Again, while applicant prefers the particular forms of steganographic encoding detailed above, the diverse applications disclosed in this specification can largely be practiced with other steganographic marking techniques, many of which are known in the prior art. Likewise, while the specification has focused on applications of this technology to images, the principles thereof are generally equally applicable to embedding such information in audio, physical media, or any other carrier of information.

Finally, while the specification has been illustrated with particular embodiments, it will be recognized that elements, components and steps from these embodiments can be recombined in

different arrangements to serve different needs and applications, as will be readily apparent to those of ordinary skill in the art.

POINTER TO A HEADER, AND/OR, POINTER TO A PROCESS

The basic philosophy surrounding the use of a "header" in a digital file has already been discussed, along with the idea that steganographically encoded information can serve many of these functions independently or in parallel with a traditional header. This section attempts to further clarify this notion as well as further clarify the notion that attached information can act as a "pointer" to a remote database containing the information that might be otherwise contained in a header. Refer to the sections on header verification, the "bodier", and network linking methods and hot objects in general. This section also expands upon the idea that header information and other kinds of attached information can be more than simply passive descriptive information, but can be fully executable code or other forms of "active information and network links."

As previously developed in the section on hot objects, given that realtime connection of a desktop computer, a television set or a stero system onto a network is becoming more and more commonplace, the absolute need for an attached header replete with full information about a data object is diminishing, and the possibility of simply pointing to a remote yet connected database is becoming more and more practical. The persistent and immediate connection to the information is more fundamental than strictly needing the full information attached to the data object (where time to change information presents a particular problem for object-attached information).

Referring back to Fig. 16, and harkening back to the discussion on networked linking methods, we find the situation depicted in Fig. 60. The header information "joe's image" is now only located on some accessible remote database, and the information attached to the object in either the actual header, or steganographically embedded, or both, now contains simply an address to the remote database location. Software applications would then be manufactured such that a networked connection would be assumed to be either active or capable of becoming so rather swiftly, and that

when a data object such as an image or a video clip was read in, the embedded address of the header information would be read, a quick retrieve of the database information would be performed, and the remote header information would be used just as if it were locally attached to the data object.

It is important to note that the stegonographic embedded information does not necessarily need to be present in order to make such a system function, and vice versa, the traditional header need not be present if steganographic information is present. The two together represent a value-added redundancy and greater assurance that the link between the remote information and the object remain intact. Likewise, even if there does exist some "master remote header" for a given data object, an "static-in-time copy" (by definition) of that master header file can still travel with the data object for the purposes of speed or for the purposes of servicing non-networked sties or applications, with reference back to the master if need be for any latest updates. Likewise, though the principles of this application focus largely on audio-visual signals and data objects, many of these design principles apply to text files, software programs, basic data records, and the like, where steganography per se may not even be applicable. Likewise, any other kind of information can certainly still be attached to an object in addition to the above mentioned "header" information. Another way to look at it is that this new "header address" can simply be appended to or incorporated into any existing header format such as JPEG, TIFF, etc.

It is also important to note that the information stored remotely need not simply be "passive information" such as a person's name or the latest price for some peddled item. It can also be computer instructions or software executable code that is associated with the data object. Thus a software application can read in a data object, reading at the same time the remote database address, retrieve via a network the remote connection, then either display the remote information along with the data object information itself, or actually launch some local application much like JAVA based systems currently function, or the remote database can actually ship executable code which may then be invoked locally on the machine where the data object has been read. In this fashion, a data object becomes a first stepping stone into some computing experience usually related to the content of the object itself, much as a cover of a book is a quick visual summary of the book's content where the challenge becomes enticing

third parties to enter.

The notion of a singular string of attached bits referring to a remote database wherein a master header is located we shall henceforth refer to as an "identity pointer". We shall refer to the database location containing the master information connected with that data object as the "master identity."

As is well known even in the prior art of traditional mail, addresses can be hierarchical in nature, with ever finer levels of granularity in searching for the ultimate central location or master identity. So too with identity pointers, they can actually be a single string of hierarchical information parsed according to where an application or machine needs to go in order to retrieve the full information associated with the data object and/or audio/visual signal. Thus, a sub-string inside the identity pointer might indicate, through proper programming of an application or instrument including address redirection tables, that the master identity for such and such object exists inside one's own computer at such and such directory and in such and such file. On the other hand, a first section of the identity pointer might indicate a search is required on the world wide web for a particular rights management database or commerce server database, a second section of the identity pointer then "points" to an address at this particular database, wherein what is pointed to may be the ultimate location of the master identity, or the pointed-to location is actually a database of further pointers to a multitude of databases, indicating that a third section of the identity pointer now has an address location of the ultimate master identity. This formula can clearly recurse further into fourth, fifth, and so on layers. The point is that it is not strictly required to have the identity pointer only point to some singular master database, but that there will in fact be a multitude of interconnected databases which will be the rule rather than the exception. This includes databases which are more traditionally viewed as belonging in some kind of network which is not necessarily as large as the internet, such as local area networks, or even a personal computers series of hard drives, or whatever. The main overall point is that the identity pointer contains sufficient information in order to be able to find the master identity, where it is a given that an application or instrument can read the master pointer, interpret it, and do the searching and retrieving of the master identity.

Those skilled in the art may notice that so far in this section no mention has been

made about encrypting either the identity pointer or the master identity or any communications involved in the overall process. Such improvements can certainly be made and enhance more of the "secure identification" aspects of an attached information system, or the related "verification" function that many commerce applications will be seeking. The basic principles of the invention can nevertheless be followed.

The identity pointer can also point to locations which are not (currently) viewed as strictly a database. For example, a data object can contain a sub-string which points to a particular application that needs to be launched in order to resolve the remainder of the identity pointer string. A more specific example of the general example might be that a sub-string in the identity pointer instructs a machine to launch a web browser, and the remainder of the string would be a traditional URL to some web page containing basic contact information to the creator of a video production. Users on a local machine might program the machine to their own liking in that they would "allow" content with these abilities to go ahead and launch browsers when instructed, or they can tell their local machine to ignore these requests by a given piece of content. Likewise, an sub-string in the identity pointer might instruct a multimedia database interface program to be launched and the location of the object in question sought, found, and displayed.

It can be readily seen that the general principles of the invention would indicate that applications and instruments which deal with data objects require less and less local intelligence regarding "interpreting and operating upon" attached information, yet instead they become better and better at being realtime connected to a broader network and know how to properly find and retrieve information from various locations on that broader network. Moreover, applications and instruments so enabled would also make use of well-known-in-the-art methods of launching new execution threads or entire new applications based on the retrieved information. The physical location of the master identity, as well as the "level" it exists on in the network hierarchy (from CPU RAM, through Operating System, through local storage disks, through local networks, up through global networks such as the Internet) becomes immaterial so long as an application or instrument is equipped with the realtime ability to find and retrieve the pertinent information.

We now turn toward a more detailed description of the drawings. Fig. 60 depicts

the essential concept behind the "master identity object" and a system built around it. ("Master Identity Object", or MIO, is here used as a convenience and should not be construed as limiting the kind of information pointed to by an embedded pointer; i.e., the MIO could easily point to executable code or executable sequences for example rather than identity information). Indeed, the system is essential to the definition of the object. Quite simply, a header is replaced by a pointer to a header, and the header information itself is located in some accessible location. The pointer 1690 represents whatever complete address information is needed in order for an instrument or application to locate the header information, 1694, located in some binary storage location (or database) 1692. The data stream 802 is whatever normal data that might be contained in a typical digital image file or binary record or software program or whatever. The pointer, 1690, can also be embedded steganographically as depicted, or alternatively, it can ONLY be associated with the data stream steganographically.

Fig. 61 begins to dissect Fig. 60, trying to depict a closer view of a practical MIO ("master identity object"). Reverence is paid to the idea that common data objects and common data formats will be used for some time to come, and in many ways the MIO information will be appended. Thus we start with a traditional header 1700 and the associated data stream 802. The MIO pointer is now split out into three pieces, a "tag" which identifies the following information as a pointer to a remote database. The pointer is now conveniently split into a pointer to a pointer 1704, effectively giving the address of some database in a sea of potential databases, while pointer 1706 is the ultimate address on the found database pointed to by 1704. Indeed, 1704 could also be split out, just as in surface mail type addressing.

Fig. 61 also indicates that multiple layers of MIO information can be added to an object. One example of this would be that an organization would track and account for all incoming and outgoing data objects and wish to provide a pointer to that given objects lifetime within the organizations data network, yet respect any previous MIO information that the creator or distributor of a data object already attached to that object. There are numerous other examples, including derivative work applications or situations where a data object evolves.

Fig. 62 takes a closer look at the connectivity components of an MIO system, looked at through the eyes of an instrument or application needing to retrieve the master

identity information for a given MIO-enabled data object. An arbitrary data object 1710 enters a highly genericized "node" 1712. Typically, this node might be an "open file" procedure in a software application, or it might be a "search for all image files" operation initiated in a computer's operating system, or it might be a digital receiver in a television set.

The node 1712 is meant to represent the place where a given data object enters a given instrument or application and is scanned for MIO traits. The node 1712's output is simply that the data object either is or is not an MIO type object. If it discovers an MIO object as in 1716, it must next ask the simple question of whether or not the given instruments cares or not, essentially asking whether or not to go fetch the information pointed to by the embedded pointer. If it is not configured to do so, it goes on with its work, 1718. If it is configured to go fetch the associated remote information (1720), it then simply goes through a basic address resolution process to locate the master identity. A first low level search might be typical wherein the "master identity" (which we have amply explained might actually be a search for further instructions rather than only "looking for a name") is potentially found on a user's own desktop computer or local instrument. This might be as low level as a call to some memory location in the CPU system 1724, perhaps retrieving and therefor instigating instructions to prepare for video information to follow. Or it might be a pointer 1726 to some location in a display device, perhaps as a precursor to understanding the current display settings that a user is operating under.

The need for multiple layers of MIO information as depicted in Fig. 61 becomes more apparent in these examples as well, in that the lower level retrieving will often be precursors to more advanced actions. Likewise, an address might be found in the operating system 1728, ROM, RAM, hard drives, etc. (1730). A token indication of a firewall 1732 is depicted showing that some addresses will only be accessible to a "local object" by design. Finally, perhaps the more common use of true "identity" will come from a route to a broader network 1734. Depicted is a certain remote database 1736 where the given data object might have its master identity. These two basic ideas of "local" identity and "remote" identity are depicted below as 1738 and 1740, but it should be appreciated that these can become quite blurry in their distinctions.

It should be understood that one object of this invention is that, for many

practical systems, the locating process of finding and retrieving the master identity information or instructions is meant to take place in realtime, that is, is typically less than a second or two ideally, and no more than ten seconds or twenty seconds even in case where there is in the multiples of kilobytes to retrieve. This kind of time performance is generally possible today on the internet even with sub-100Kbit per second modems, though less than a second is generally out of reach of current modem-based systems using standard phone lines and standard internet communications protocols.

Fig. 63 traces out a generic process flow within an instrument or application with a slightly different twist than depicted in Fig. 62. Again, any device capable of processing a data object reads said object in, 1750, and asks the simple question of whether or not remote associated information exists for that object 1752. If not, fine, 1754, go about your way. If so, it asks should I care, 1758, if not (1760, go about your way. If so, 1762, go fetch the information (or series of information if there is recursive MIO information). Box 1766 then explicitly shows that the user's device will still effect what happens even after the remote data is retrieved.

The permutations and combinations of operations from this point forward are as broad as general computing principles permit. As one tiny example, the user may have configured the device such that if the retrieved information does not match certain "key words" that the user has chosen, then don't even bother displaying an image (assuming that is the data object in question). Essentially, the retrieved information from 1764 and the user configuration 1766 set up a generally unlimited set of new instructions to the device. Another example might be that the user configuration 1766 says to go ahead and follow whatever instructions come back with the retrieved information, such as "launch a browser and follow an URL to some JAVA web site and don't mind sending out my credit card information if they ask". This is deliberately melodramatic to illustrate that the basic branching at 1770 is as broad as general computing principles permit.

Fig. 64 briefly illustrates that both embedded information as well as pointed-to information can actually sequences of instructions, including decision branched instructions, not merely singular instructions or singular blocks of passive descriptive information. This idea is encapsulated in the word "script" as is generally well known

in the art of computing.

Fig. 65 essentially depicts an MIO system operated in "reverse" from that of the previous few figures. In general, the idea here is that the master identity wants to know and collect all migration activities of its associated data object, and the system depicted in Fig. 65 is essentially a way to do this. Again, we see a generic data object 1820 entering some generic application or instrument 1822, here referred to as a "reporting node". The first question still is "are you an MIO?" 1824. 1826 alludes to the idea of reporting non-hits to some kind of master MIO system database 1830, a database which might track the broad traffic patterns of MIO object vs. Non-MIO objects. If the node finds an MIO, the next logical question is "may" I send a message to its master identity in order to inform the master identity that this object passed this location at this particular time? (1834). This is important since there will be many situations due to privacy and security considerations where such reporting would be intolerable 1834. However, there may also be many situations where this reporting information is valuable to all users of MIO based systems, and a "count" message will be sent to the master identity location, where locating the master identity follows previous descriptions. Details of how the master identity collects messages are left silent here as this form of data collection technology is readily available in today's marketplace and computing systems, where ultra-mundane methods such as sending a self-contained e-mail to some e-mail address might even suffice as a methodology of counting (horribly inefficient but indicative of the vast arrays of methods to have a master identity database keep track of hundreds if not millions of copies of "itself").

In view of the wide variety of implementations and applications to which the principles of this technology can be put, it should be apparent that the detailed embodiments are illustrative only and in no way limit the scope of my invention. I claim as my invention all such embodiments as come within the scope and spirit of the following claims and equivalents thereto.

CLAIMS

1. A multi-computer system including a network for embedding and reading a watermark, the system comprising:

a first digital electrical computer system comprising a first digital electrical computer electrically connected to a first input device, to a first output device, and to a first memory storing a plurality of creator identifiers and creator contact data corresponding to each of the creator identifiers;

a second digital electrical computer system comprising a second digital electrical computer electrically connected to a second input device and to a second output device, the second digital electrical computer being programmed to embed a watermark in a digital photographic image, the watermark including one of the plurality of creator identifiers;

a third digital electrical computer system comprising a third digital electrical computer electrically connected to a third input device and to a third output device, the third digital electrical computer being programmed to read the watermark in the digital photographic image to reveal the one of the plurality of creator identifiers;

a network for communicating the revealed one of the plurality of creator identifiers to the first digital electrical computer to obtain the creator contact data corresponding to the one of the plurality of creator identifiers form the memory.

2. The system of claim 1, wherein:

the second digital electrical computer is programmed to automatically detect for a watermark when an image is first examined by the second digital electrical computer.

3. The system of claim 1, wherein:

the second digital electrical computer is programmed to selectably detect for a watermark when an image is examined by the second digital electrical computer.

4. The system of claim 1, wherein:

the network includes the Internet;

the watermark includes information identifying a World Wide Web site; and

wherein

the third digital electrical computer system is programmed to load a World Wide Web browser and connect to the World Wide Web site in response to the revealed one

of the plurality of creator identifiers.

5. The system of claim 1, wherein:

the watermark includes extended data including at least one member from the group consisting of an organization identifier, a transaction identifier, and an item identifier.

6. In a television set, audio stereo system, computing system, or other system capable of receiving, storing, transmitting, or processing an audio or visual signal, an improvement comprising:

means for adding to an initial audio or visual signal an additional digital information associated with the initial signal,

the additional information containing, in whole or in part, an identification number which is uniquely assigned to the individual initial signal or copies thereof,

wherein the identification number represents an address to a location in a remote database wherein a prestored set of information associated with the initial signal is contained, and

means coupled to the system containing a processor responsive to basic operating instructions for enabling the reading of the additional information and enabling the realtime retrieving from the remote database a subset of the prestored information via a communications link with the remote site.

7. The system of claim 6, wherein the prestored set of information comprises identification and description information about the signal or an object contained in or represented by the signal.

8. The system of claim 6, wherein the prestored set of information comprises a set of machine instructions executable to perform a task relative to the initial signal or about an object contained in the initial signal.

9. The system of claim 6, wherein the prestored set of information comprises a menu of options or commands.

10. The system of claim 1, including means for steganographically embedding the additional information in the initial signal.

11. The system of claim 1, wherein there also exists a second number as part of the additional information, wherein the second number is the address or identifier of the database itself to which the first identification points inside, in the context of

multiple databases serving a multitude of audio and visual signals.

12. The system of claim 4, first and second numbers steganographically embedded in the initial signal.

13. The system of claim 1, wherein there is additionally an instrument or receiving station which monitors a multiple number of audio/visual public channels searching and recording the identification numbers and reporting sitings.

14. In an image processing method that includes steganographically decoding an input two-dimensional image to extract a multi-bit code therein, the image comprising a two-dimensional array of pixels, an improvement comprising:

transforming the image into the spatial frequency domain;

pattern matching the transformed image so spatial frequencies obtained by said transforming step coincide with reference spatial frequencies, to thereby effect registration of the transformed image;

inverse-transforming the transformed image to yield a registered image;

identifying, in the registered image, a plurality of regions that encode a first control bit, said regions being distributed through the registered image in a regular array;

performing a statistical analysis over at least said plurality of regions to determine whether the first control bit has first or second values;

if said control bit has the first value, performing a first decoding process on the image to extract the code therefrom; and

if said control bit has the second value, performing a second decoding process on the image to extract the code therefrom, the second decoding process being different than the first.

FIG. 1

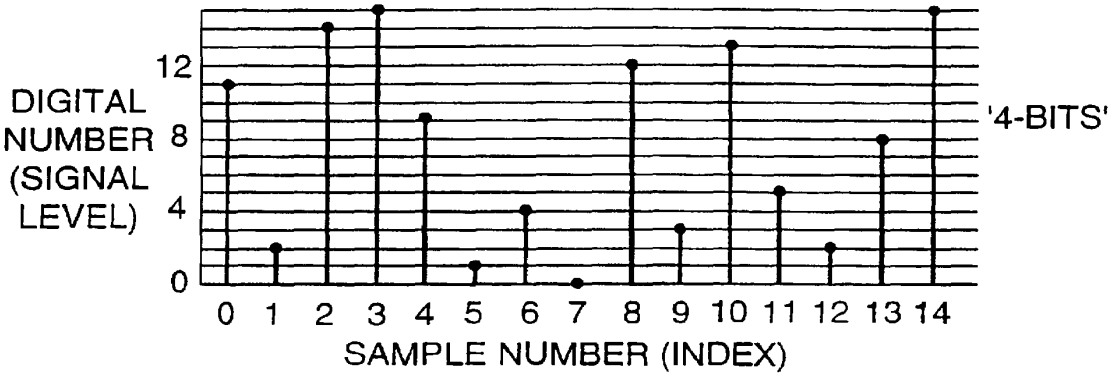

DIGITAL NUMBER (SIGNAL LEVEL)
12
8
4
0
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
SAMPLE NUMBER (INDEX)
'4-BITS'

FIG. 4

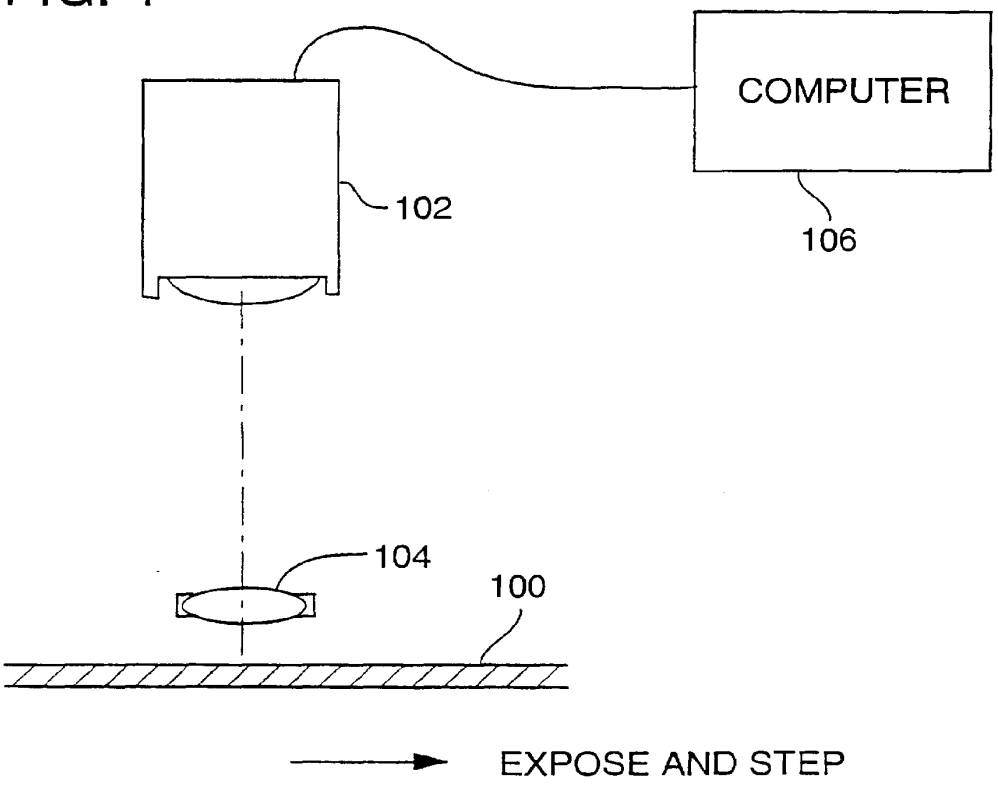

COMPUTER
102
106
104
100
EXPOSE AND STEP

FIG. 2

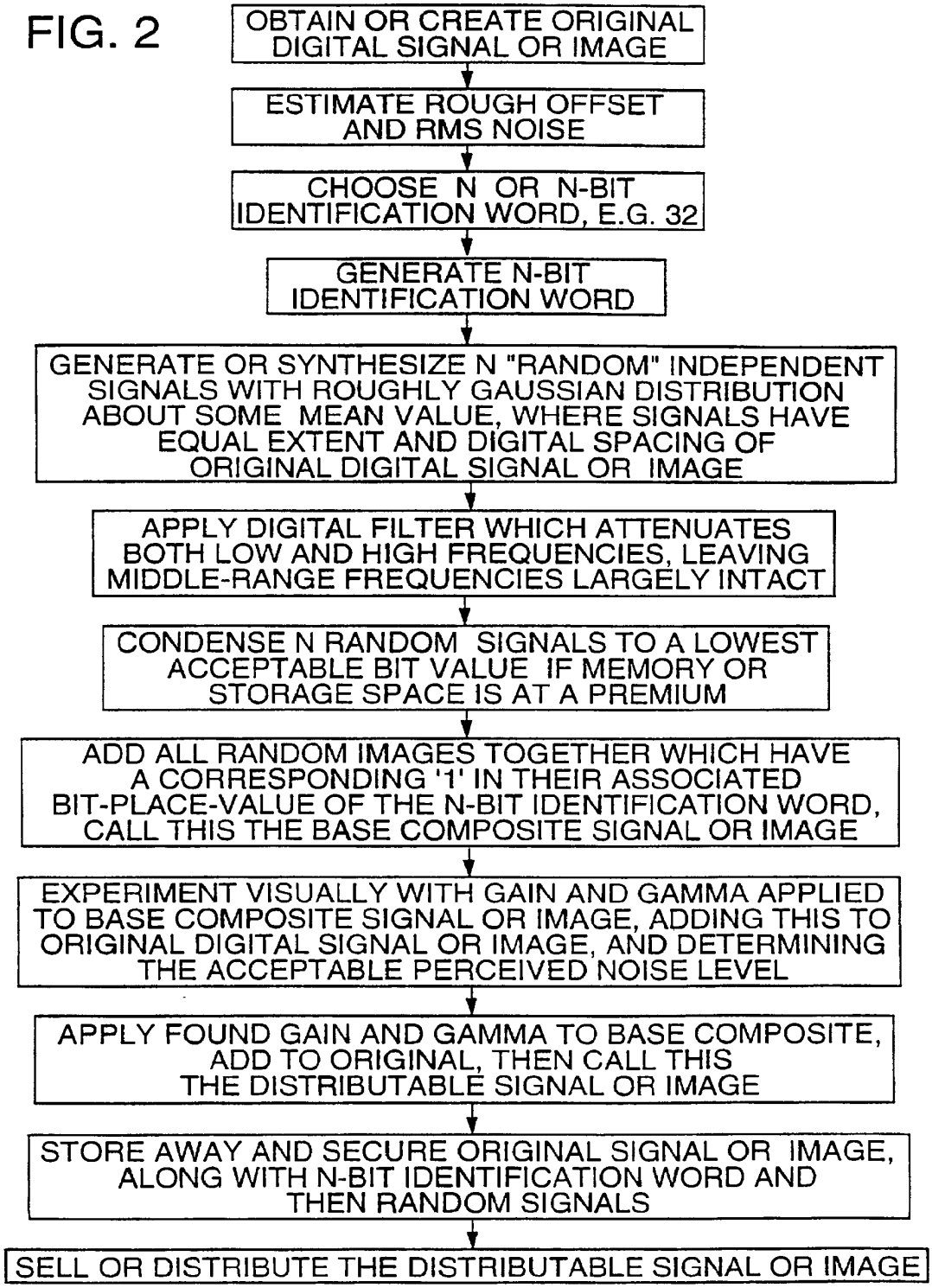

OBTAIN OR CREATE ORIGINAL DIGITAL SIGNAL OR IMAGE
ESTIMATE ROUGH OFFSET AND RMS NOISE
CHOOSE N OR N-BIT IDENTIFICATION WORD, E.G. 32
GENERATE N-BIT IDENTIFICATION WORD
GENERATE OR SYNTHESIZE N "RANDOM" INDEPENDENT SIGNALS WITH ROUGHLY GAUSSIAN DISTRIBUTION ABOUT SOME MEAN VALUE, WHERE SIGNALS HAVE EQUAL EXTENT AND DIGITAL SPACING OF ORIGINAL DIGITAL SIGNAL OR IMAGE
APPLY DIGITAL FILTER WHICH ATTENUATES BOTH LOW AND HIGH FREQUENCIES, LEAVING MIDDLE-RANGE FREQUENCIES LARGELY INTACT
CONDENSE N RANDOM SIGNALS TO A LOWEST ACCEPTABLE BIT VALUE IF MEMORY OR STORAGE SPACE IS AT A PREMIUM
ADD ALL RANDOM IMAGES TOGETHER WHICH HAVE A CORRESPONDING '1' IN THEIR ASSOCIATED BIT-PLACE-VALUE OF THE N-BIT IDENTIFICATION WORD, CALL THIS THE BASE COMPOSITE SIGNAL OR IMAGE
EXPERIMENT VISUALLY WITH GAIN AND GAMMA APPLIED TO BASE COMPOSITE SIGNAL OR IMAGE, ADDING THIS TO ORIGINAL DIGITAL SIGNAL OR IMAGE, AND DETERMINING THE ACCEPTABLE PERCEIVED NOISE LEVEL
APPLY FOUND GAIN AND GAMMA TO BASE COMPOSITE, ADD TO ORIGINAL, THEN CALL THIS THE DISTRIBUTABLE SIGNAL OR IMAGE
STORE AWAY AND SECURE ORIGINAL SIGNAL OR IMAGE, ALONG WITH N-BIT IDENTIFICATION WORD AND THEN RANDOM SIGNALS
SELL OR DISTRIBUTE THE DISTRIBUTABLE SIGNAL OR IMAGE

FIG. 3

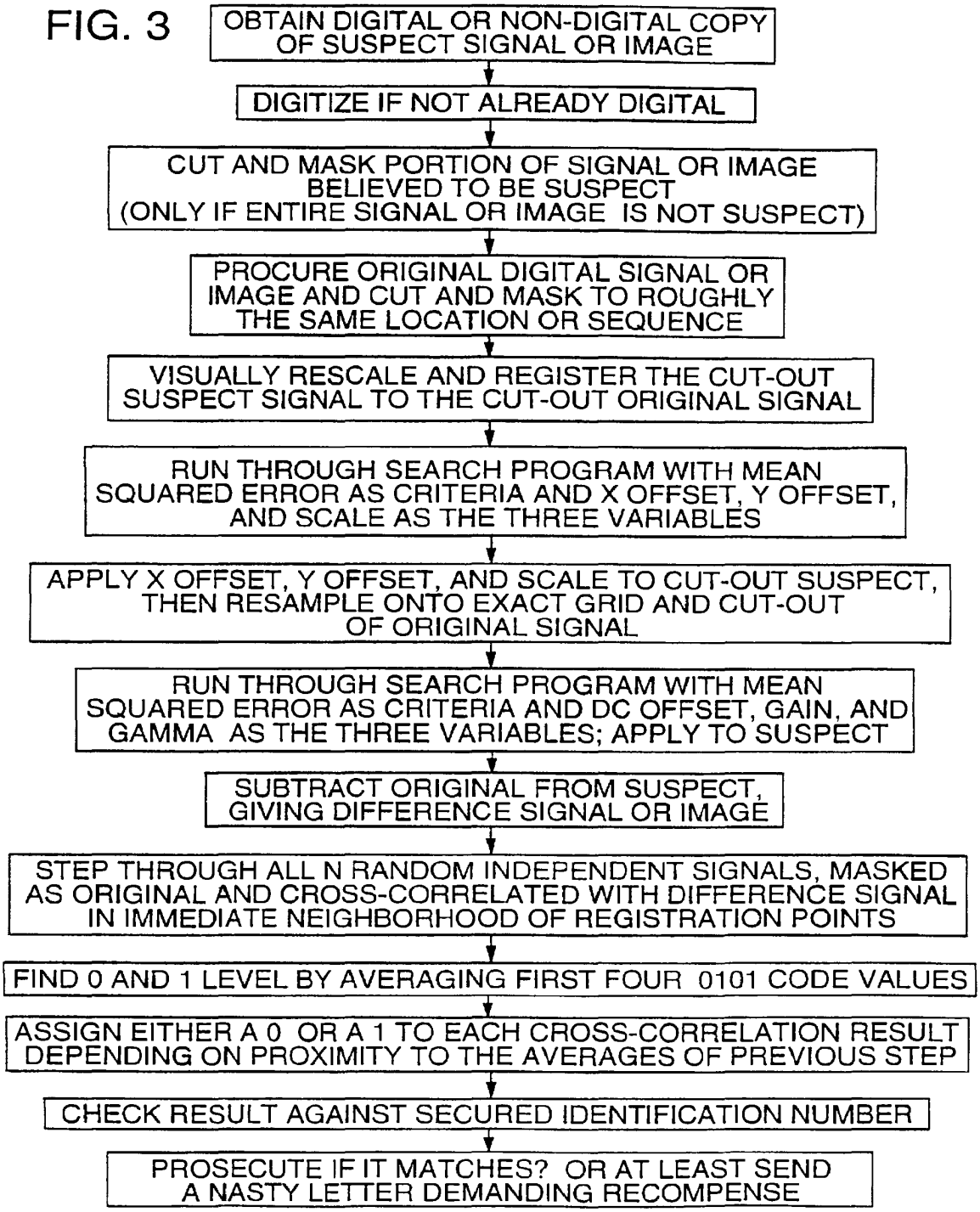

OBTAIN DIGITAL OR NON-DIGITAL COPY OF SUSPECT SIGNAL OR IMAGE
DIGITIZE IF NOT ALREADY DIGITAL
CUT AND MASK PORTION OF SIGNAL OR IMAGE BELIEVED TO BE SUSPECT (ONLY IF ENTIRE SIGNAL OR IMAGE IS NOT SUSPECT)
PROCURE ORIGINAL DIGITAL SIGNAL OR IMAGE AND CUT AND MASK TO ROUGHLY THE SAME LOCATION OR SEQUENCE
VISUALLY RESCALE AND REGISTER THE CUT-OUT SUSPECT SIGNAL TO THE CUT-OUT ORIGINAL SIGNAL
RUN THROUGH SEARCH PROGRAM WITH MEAN SQUARED ERROR AS CRITERIA AND X OFFSET, Y OFFSET, AND SCALE AS THE THREE VARIABLES
APPLY X OFFSET, Y OFFSET, AND SCALE TO CUT-OUT SUSPECT, THEN RESAMPLE ONTO EXACT GRID AND CUT-OUT OF ORIGINAL SIGNAL
RUN THROUGH SEARCH PROGRAM WITH MEAN SQUARED ERROR AS CRITERIA AND DC OFFSET, GAIN, AND GAMMA AS THE THREE VARIABLES; APPLY TO SUSPECT
SUBTRACT ORIGINAL FROM SUSPECT, GIVING DIFFERENCE SIGNAL OR IMAGE
STEP THROUGH ALL N RANDOM INDEPENDENT SIGNALS, MASKED AS ORIGINAL AND CROSS-CORRELATED WITH DIFFERENCE SIGNAL IN IMMEDIATE NEIGHBORHOOD OF REGISTRATION POINTS
FIND 0 AND 1 LEVEL BY AVERAGING FIRST FOUR 0101 CODE VALUES
ASSIGN EITHER A 0 OR A 1 TO EACH CROSS-CORRELATION RESULT DEPENDING ON PROXIMITY TO THE AVERAGES OF PREVIOUS STEP
CHECK RESULT AGAINST SECURED IDENTIFICATION NUMBER
PROSECUTE IF IT MATCHES? OR AT LEAST SEND A NASTY LETTER DEMANDING RECOMPENSE

FIG. 5

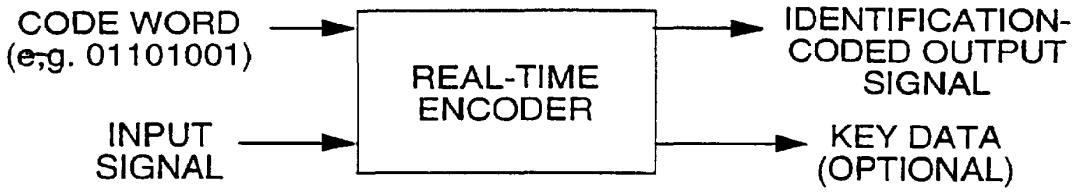
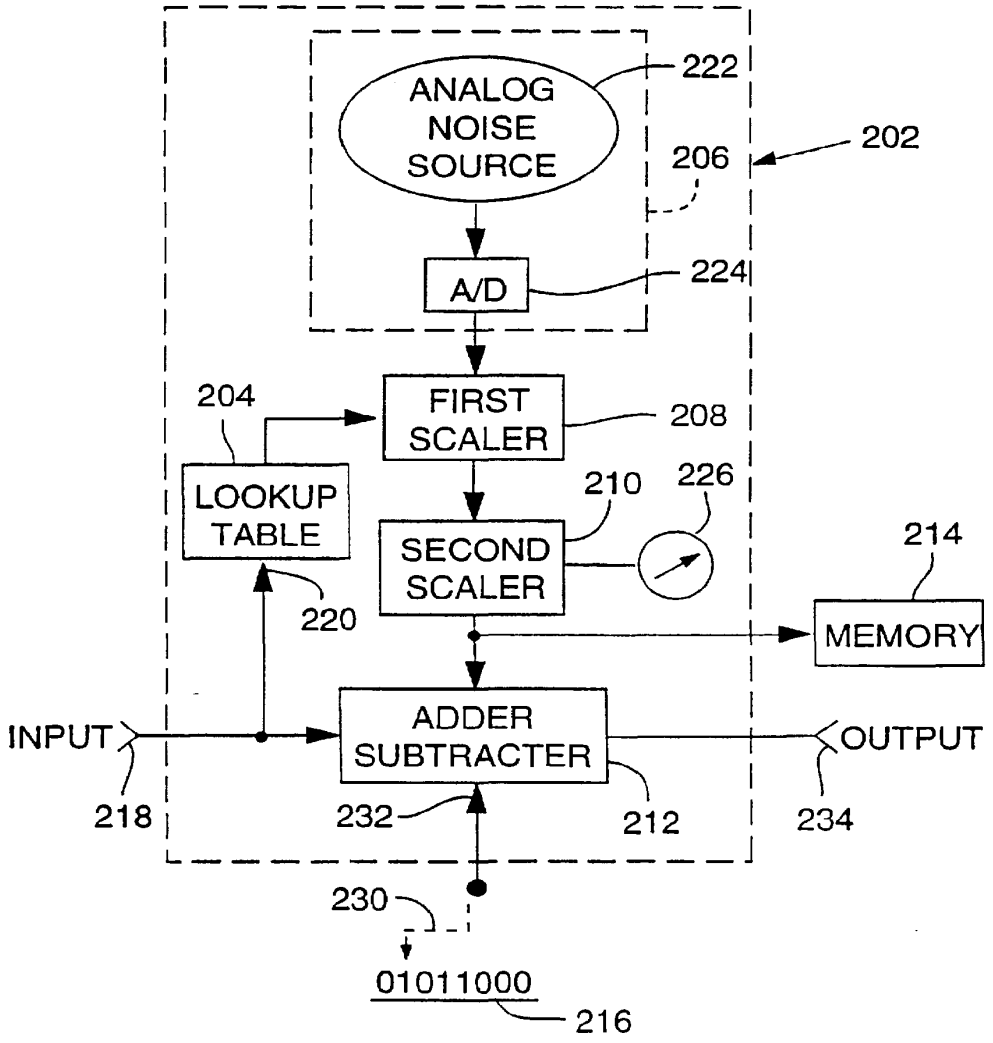

CODE WORD
(e.g. 01101001)
INPUT
SIGNAL
REAL-TIME
ENCODER
IDENTIFICATION-
CODED OUTPUT
SIGNAL
KEY DATA
(OPTIONAL)

FIG. 6


ANALOG
NOISE
SOURCE
222
206
202
A/D
224
204
FIRST
SCALER
208
LOOKUP
TABLE
210
226
SECOND
SCALER
214
220
MEMORY
INPUT
ADDER
SUBTRACTER
OUTPUT
218
232
212
234
230
01011000
216

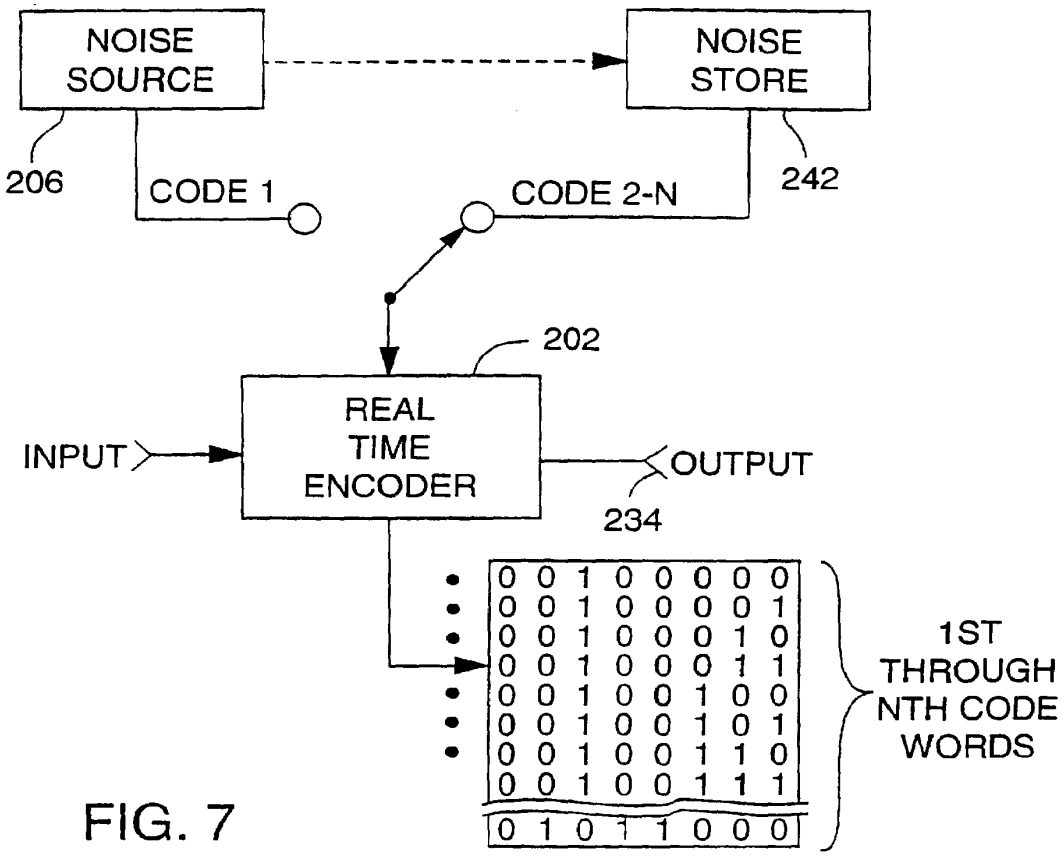

NOISE SOURCE
NOISE STORE
206
CODE 1
CODE 2-N
242
202
REAL TIME ENCODER
INPUT
OUTPUT
234
0 0 1 0 0 0 0 0
0 0 1 0 0 0 0 1
0 0 1 0 0 0 1 0
0 0 1 0 0 0 1 1
0 0 1 0 0 1 0 0
0 0 1 0 0 1 0 1
0 0 1 0 0 1 1 0
0 0 1 0 0 1 1 1
0 1 0 1 1 0 0 0
1ST THROUGH NTH CODE WORDS

FIG. 7

FIG. 8

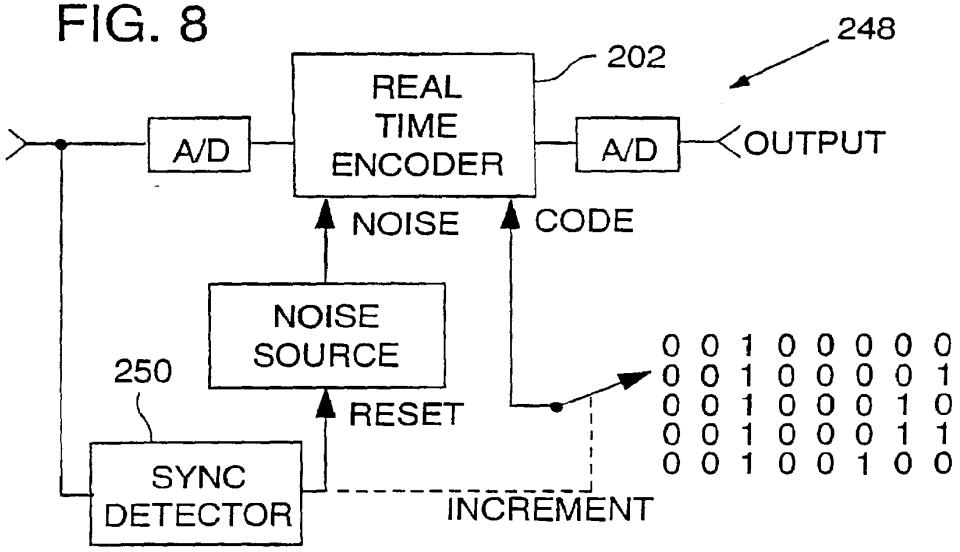

248
202
REAL TIME ENCODER
A/D
A/D
OUTPUT
NOISE
CODE
NOISE SOURCE
250
RESET
SYNC DETECTOR
INCREMENT
0 0 1 0 0 0 0 0
0 0 1 0 0 0 0 1
0 0 1 0 0 0 1 0
0 0 1 0 0 0 1 1
0 0 1 0 0 1 0 0

FIG. 9A

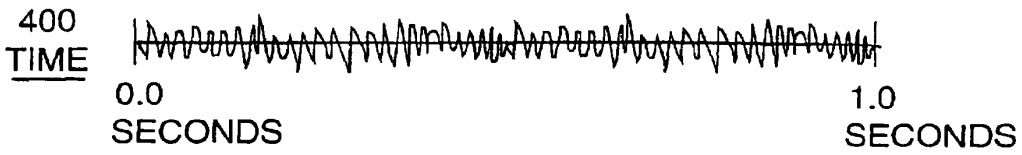


FIG. 9B

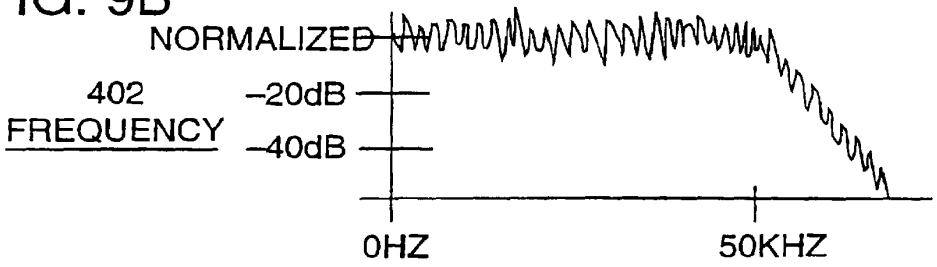


FIG. 9C

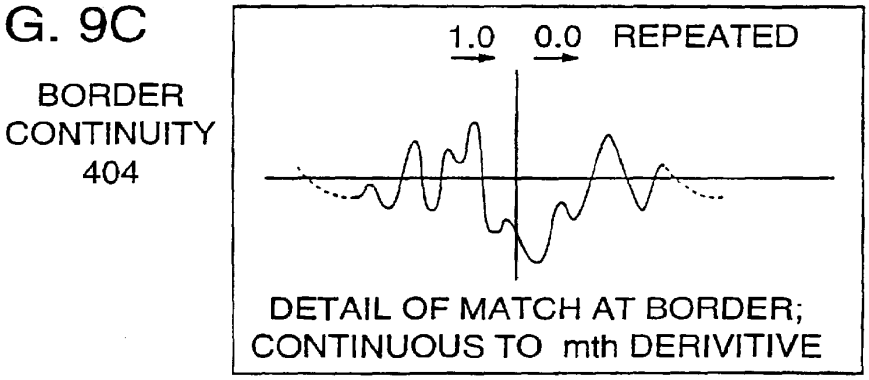


FIG. 10

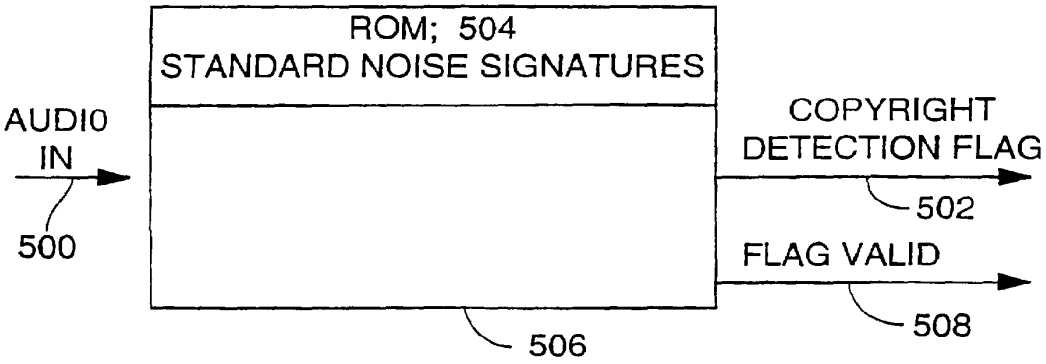


FIG. 11

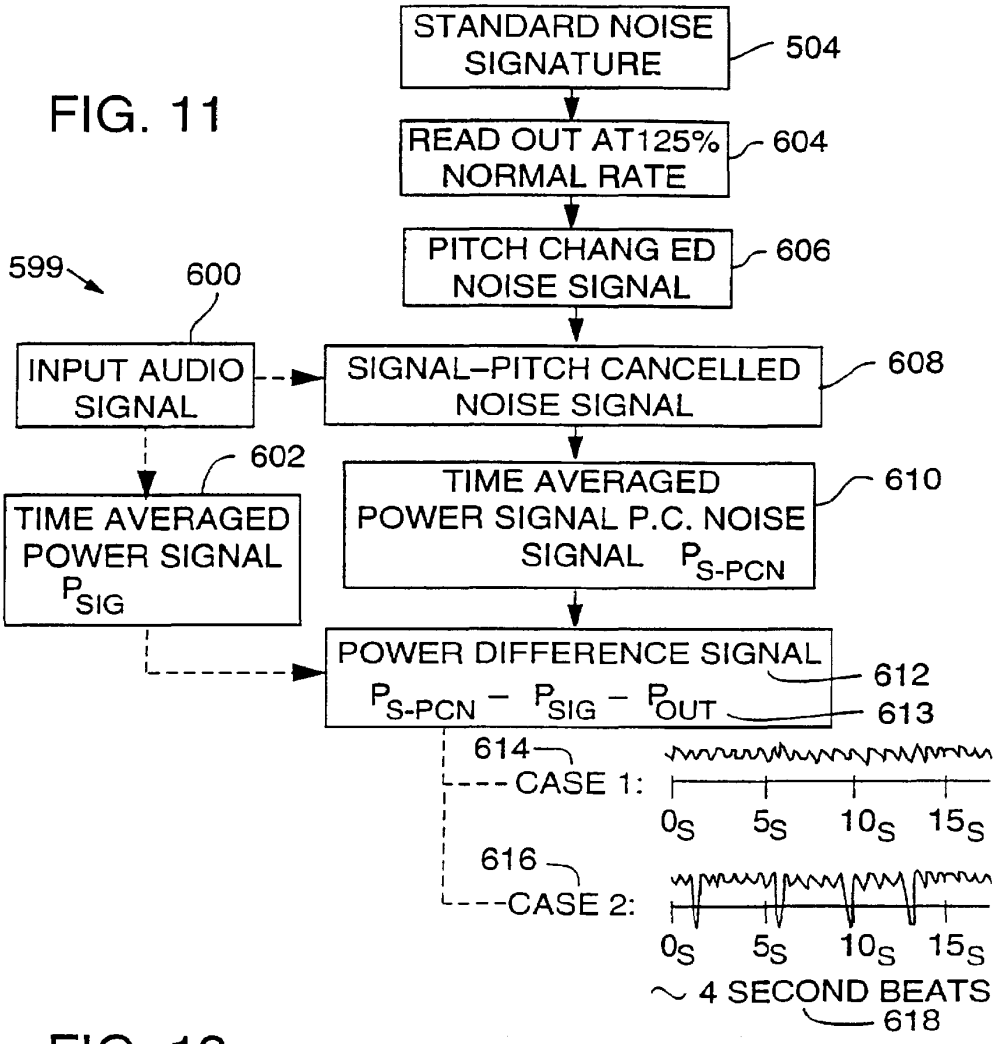

STANDARD NOISE SIGNATURE
504
READ OUT AT125% NORMAL RATE
604
PITCH CHANG ED NOISE SIGNAL
606
599
600
INPUT AUDIO SIGNAL
SIGNAL–PITCH CANCELLED NOISE SIGNAL
608
602
TIME AVERAGED POWER SIGNAL P_{SIG}
TIME AVERAGED POWER SIGNAL P.C. NOISE SIGNAL P_{S-PCN}
610
POWER DIFFERENCE SIGNAL
$P_{S-PCN} - P_{SIG} - P_{OUT}$
612
613
614
CASE 1:
0_S 5_S 10_S 15_S
616
CASE 2:
0_S 5_S 10_S 15_S
4 SECOND BEATS
618

FIG. 12

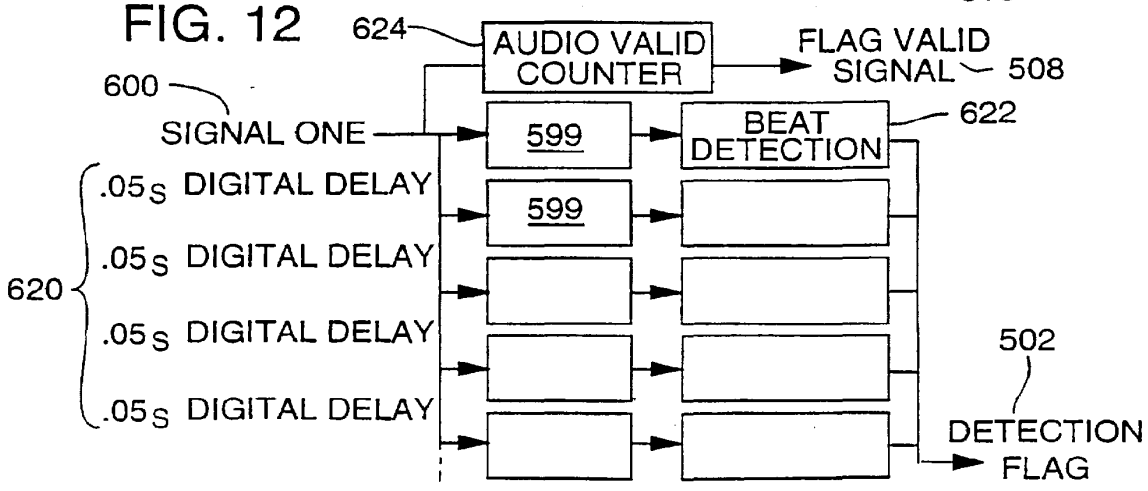
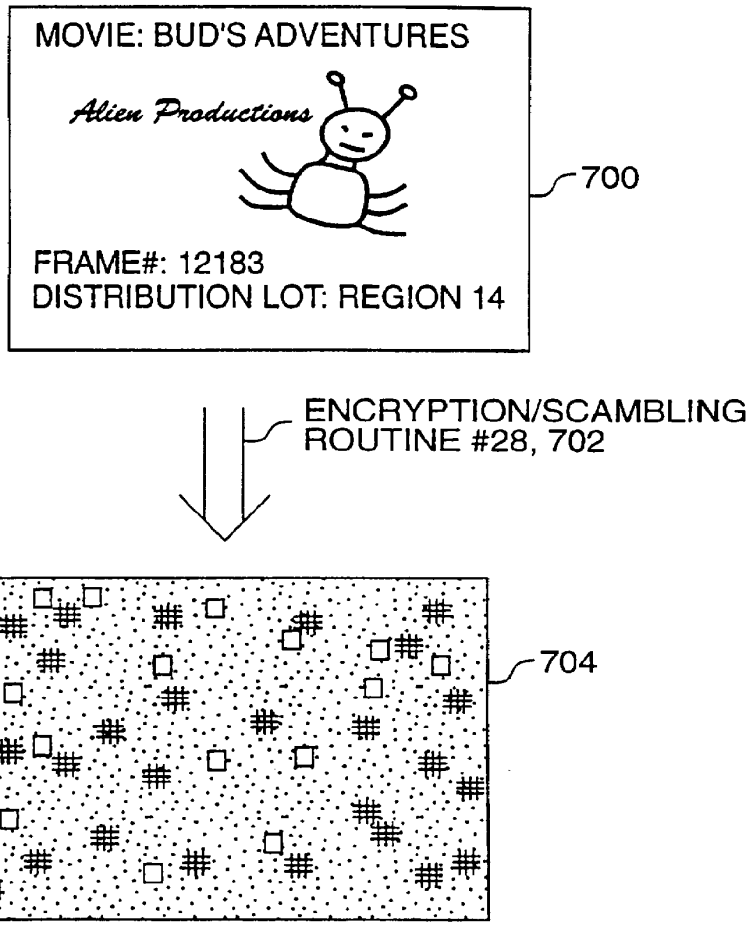
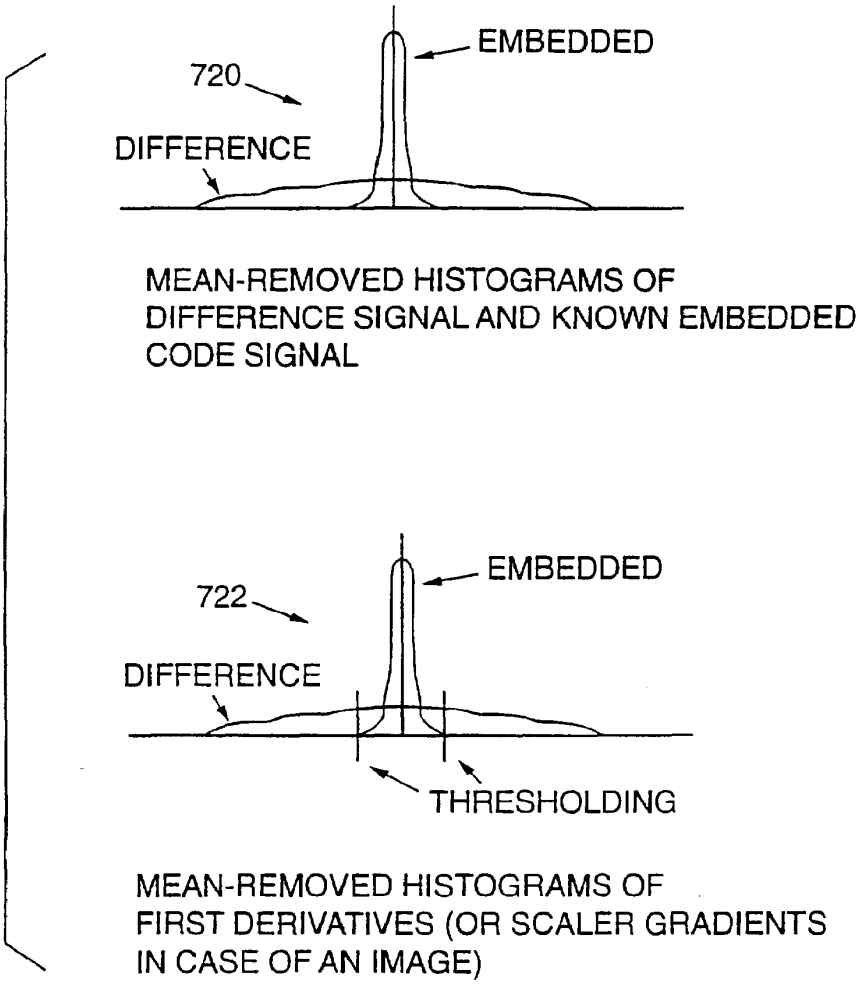

624
AUDIO VALID COUNTER
FLAG VALID SIGNAL
508
600
SIGNAL ONE
599
BEAT DETECTION
622
620
.05S DIGITAL DELAY
599
.05S DIGITAL DELAY
.05S DIGITAL DELAY
.05S DIGITAL DELAY
502
DETECTION FLAG

FIG. 13



PSEUDO-RANDOM MASTER SNOWY IMAGE
(SCALED DOWN AND ADDED TO FRAME 12183)

FIG. 14


EMBEDDED
720
DIFFERENCE
MEAN-REMOVED HISTOGRAMS OF DIFFERENCE SIGNAL AND KNOWN EMBEDDED CODE SIGNAL
EMBEDDED
722
DIFFERENCE
THRESHOLDING
MEAN-REMOVED HISTOGRAMS OF FIRST DERIVATIVES (OR SCALER GRADIENTS IN CASE OF AN IMAGE)

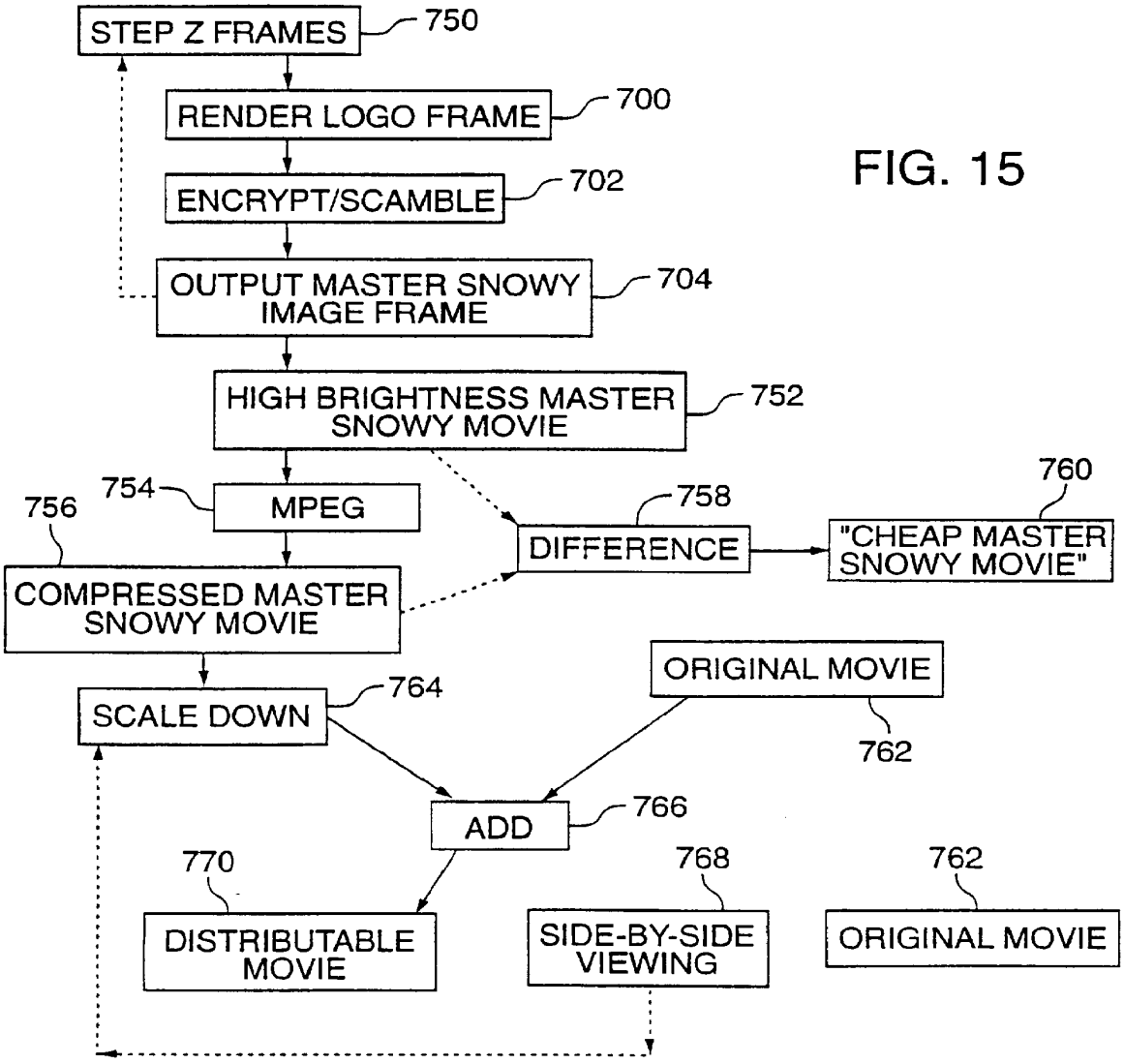

STEP Z FRAMES
750
RENDER LOGO FRAME
700
ENCRYPT/SCAMBLE
702
OUTPUT MASTER SNOWY IMAGE FRAME
704
HIGH BRIGHTNESS MASTER SNOWY MOVIE
752
754
MPEG
756
COMPRESSED MASTER SNOWY MOVIE
758
DIFFERENCE
760
"CHEAP MASTER SNOWY MOVIE"
ORIGINAL MOVIE
762
SCALE DOWN
764
ADD
766
770
DISTRIBUTABLE MOVIE
768
SIDE-BY-SIDE VIEWING
762
ORIGINAL MOVIE

FIG. 15

FIG. 16

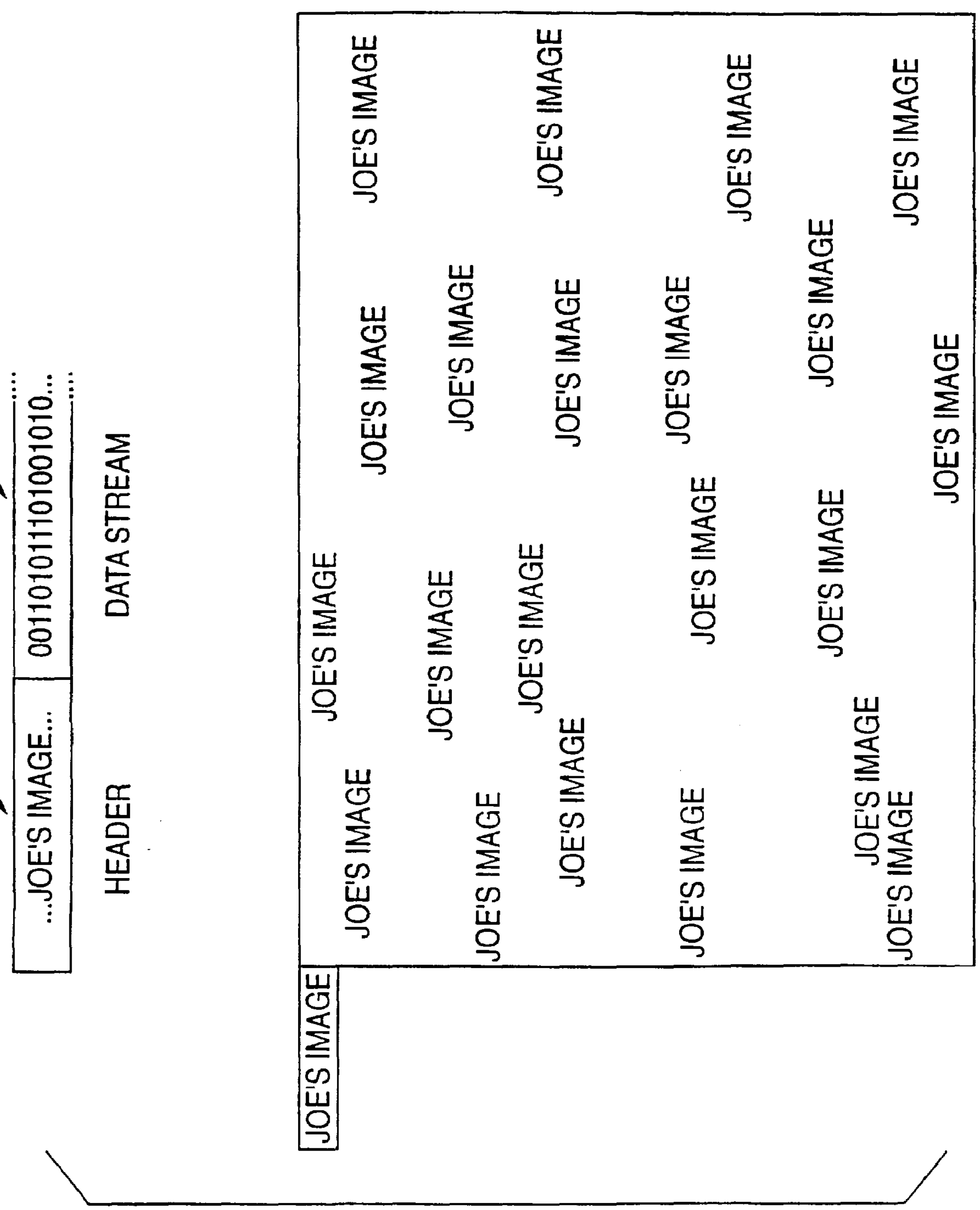
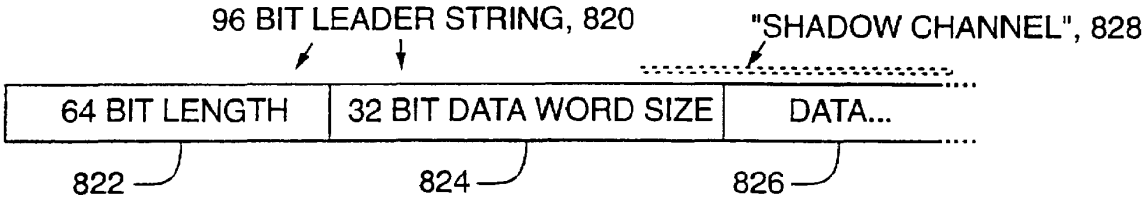

800
802
...JOE'S IMAGE...
0011010111101001010...
HEADER
DATA STREAM
JOE'S IMAGE

FIG. 17



UNIVERSAL EMPIRICAL DATA FORMAT

FIG. 18

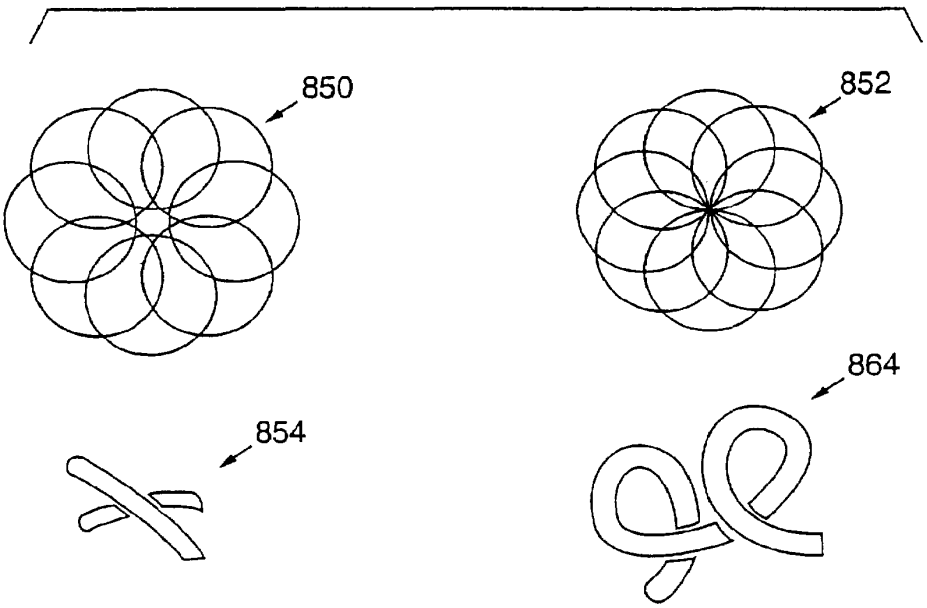
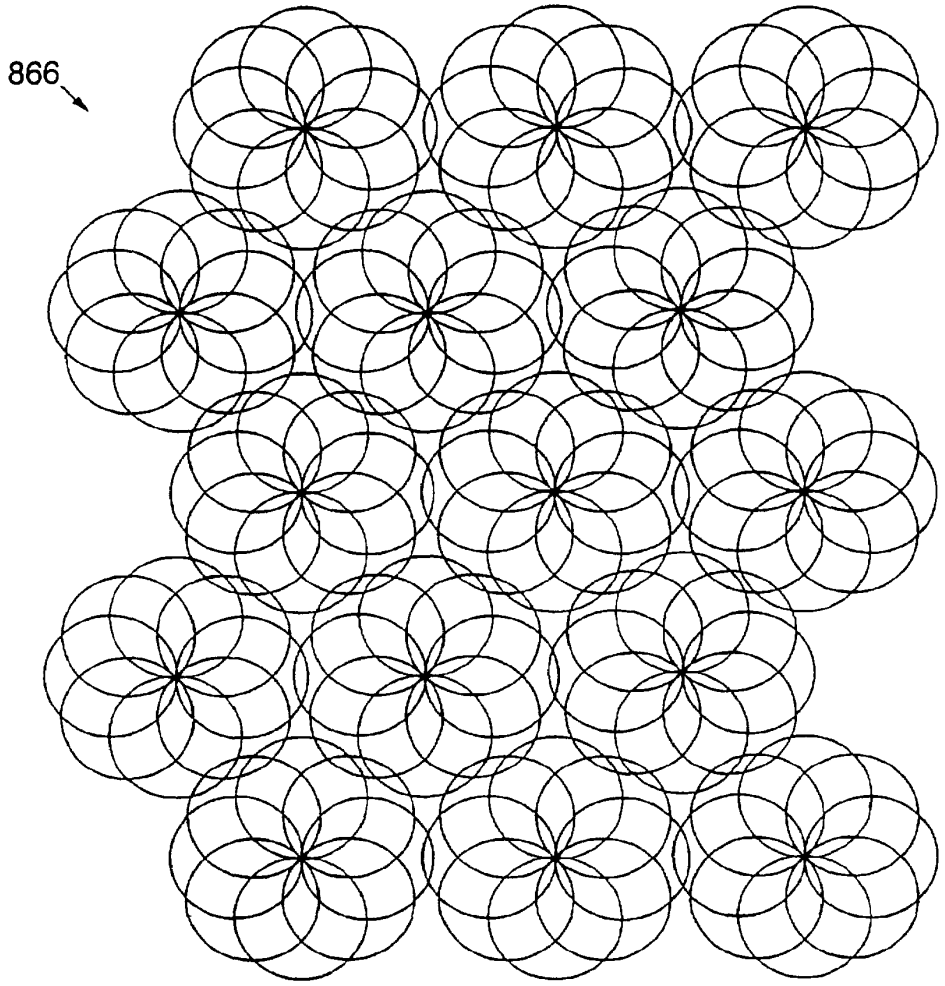


FIG. 19



QUEST FOR MOSAICED KNOT PATTERNS WHICH "COVER" AND ARE COEXTENSIVE WITH ORIGINAL IMAGE;
ALL ELEMENTAL KNOT PATTERNS CAN CONVEY THE SAME INFORMATION, SUCH AS A SIGNATURE, OR EACH CAN CONVEY A NEW MESSAGE IN A STEGANOGRAPHIC SENSE

FIG. 20

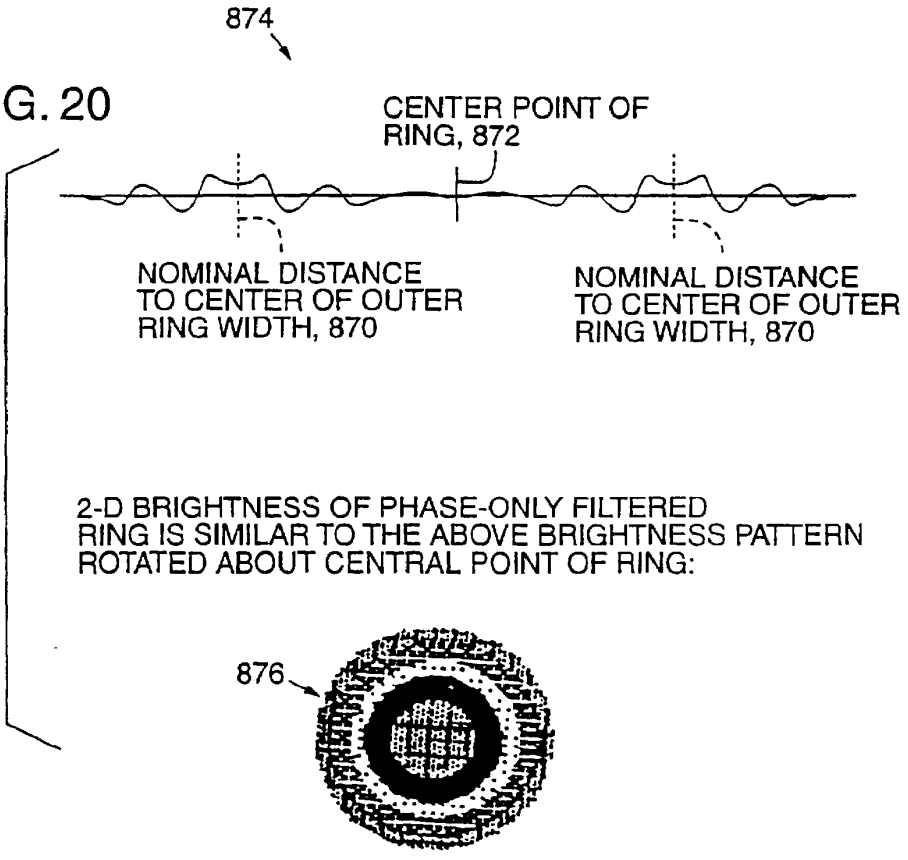

874
CENTER POINT OF RING, 872
NOMINAL DISTANCE TO CENTER OF OUTER RING WIDTH, 870
NOMINAL DISTANCE TO CENTER OF OUTER RING WIDTH, 870
2-D BRIGHTNESS OF PHASE-ONLY FILTERED RING IS SIMILAR TO THE ABOVE BRIGHTNESS PATTERN ROTATED ABOUT CENTRAL POINT OF RING:
876

FIG. 21A

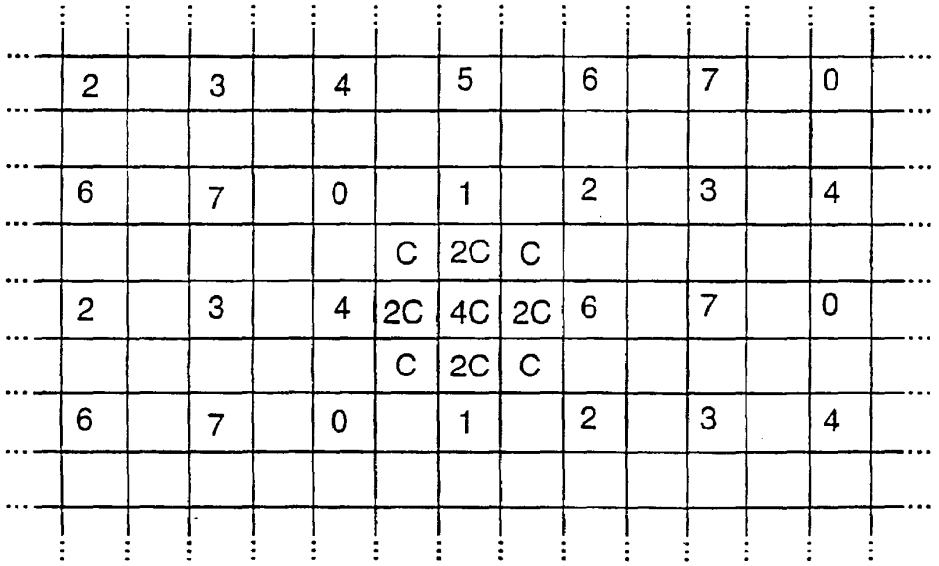
900 →

C	2C	C
2C	4C	2C
C	2C	C

WHERE C = 1/16

ELEMENTARY BUMP
(DEFINED GROUPING OF PIXELS WITH WEIGHT VALUES)

FIG. 21B



EXAMPLE OF HOW MANY ELEMENTARY BUMPS, 900, WOULD BE ASSIGNED LOCATIONS IN AN IMAGE, AND THOSE LOCATIONS WOULD BE ASSOCIATED WITH A CORRESPONDING BIT PLANE IN THE N-BIT WORD, HERE TAKEN AS N=8 WITH INDEXES OF 0-7. ONE LOCATION, ASSOCIATED WITH BIT PLANE "5", HAS THE OVERLAY OF THE BUMP PROFILE DEPICTED.

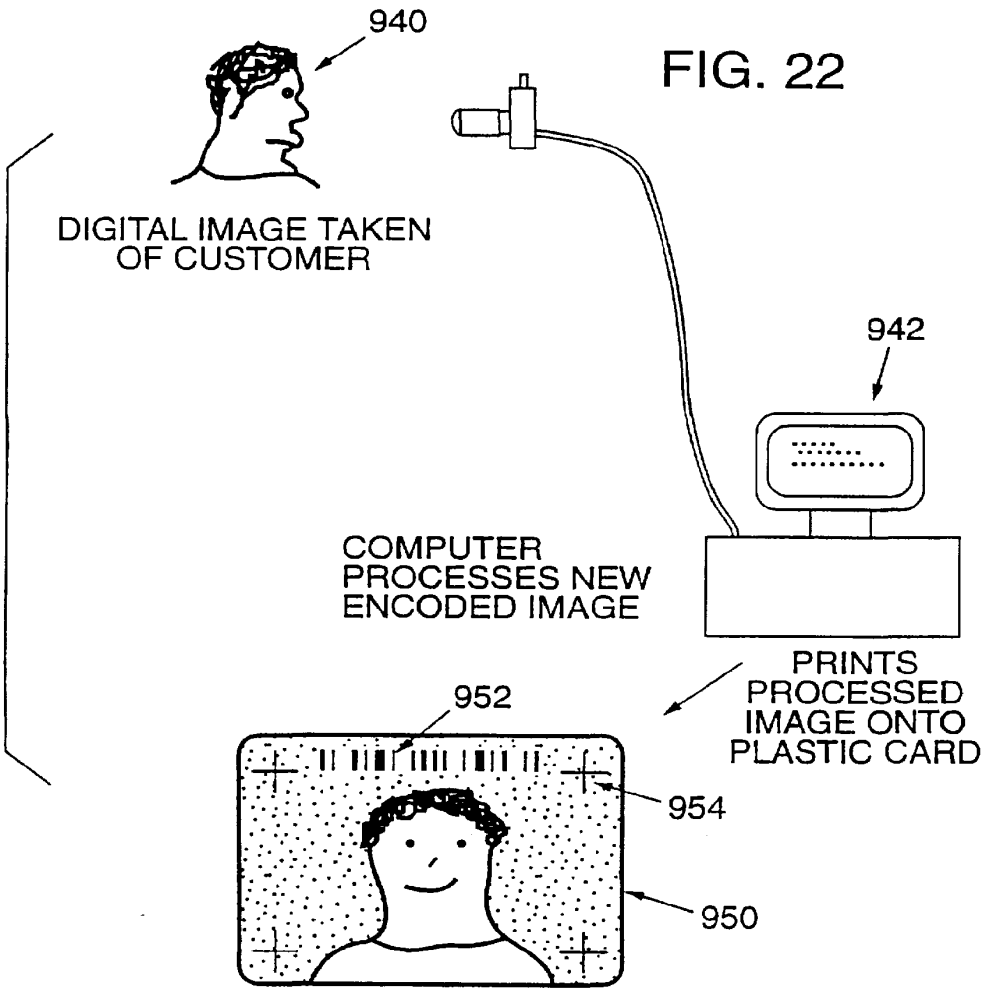
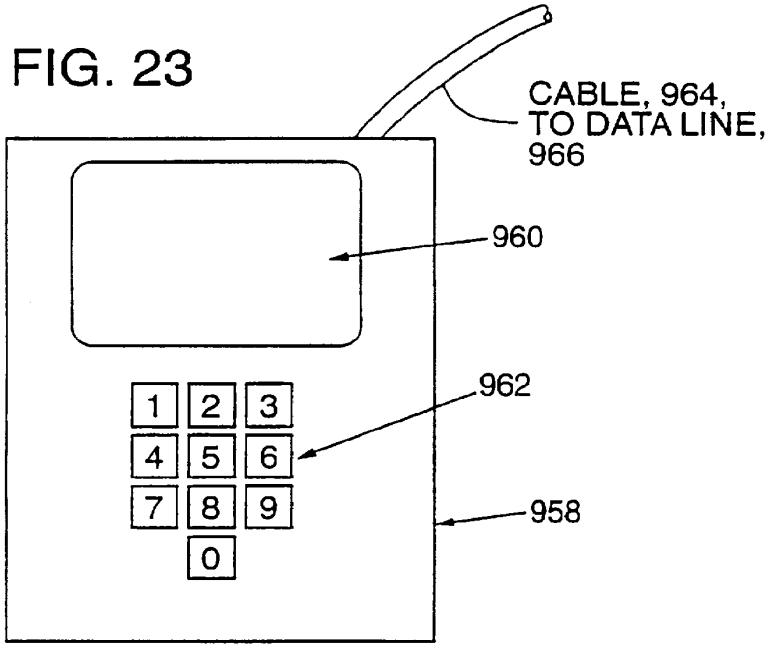

940
DIGITAL IMAGE TAKEN OF CUSTOMER
942
COMPUTER PROCESSES NEW ENCODED IMAGE
PRINTS PROCESSED IMAGE ONTO PLASTIC CARD
952
954
950

FIG. 22

FIG. 23



CONTAINS RUDIMENTARY OPTICAL SCANNER, MEMORY BUFFERS, COMMUNICATIONS DEVICES, AND MICROPROCESSOR

CONSUMER MERELY PLACES CARD INTO WINDOW AND CAN, AT THEIR PREARRANGED OPTION, EITHER TYPE IN A PERSONAL IDENTIFICATION NUMBER (PIN, FOR ADDED SECURITY) OR NOT. THE TRANSACTION IS APPROVED OR DISAPPROVED WITHIN SECONDS.

FIG. 24

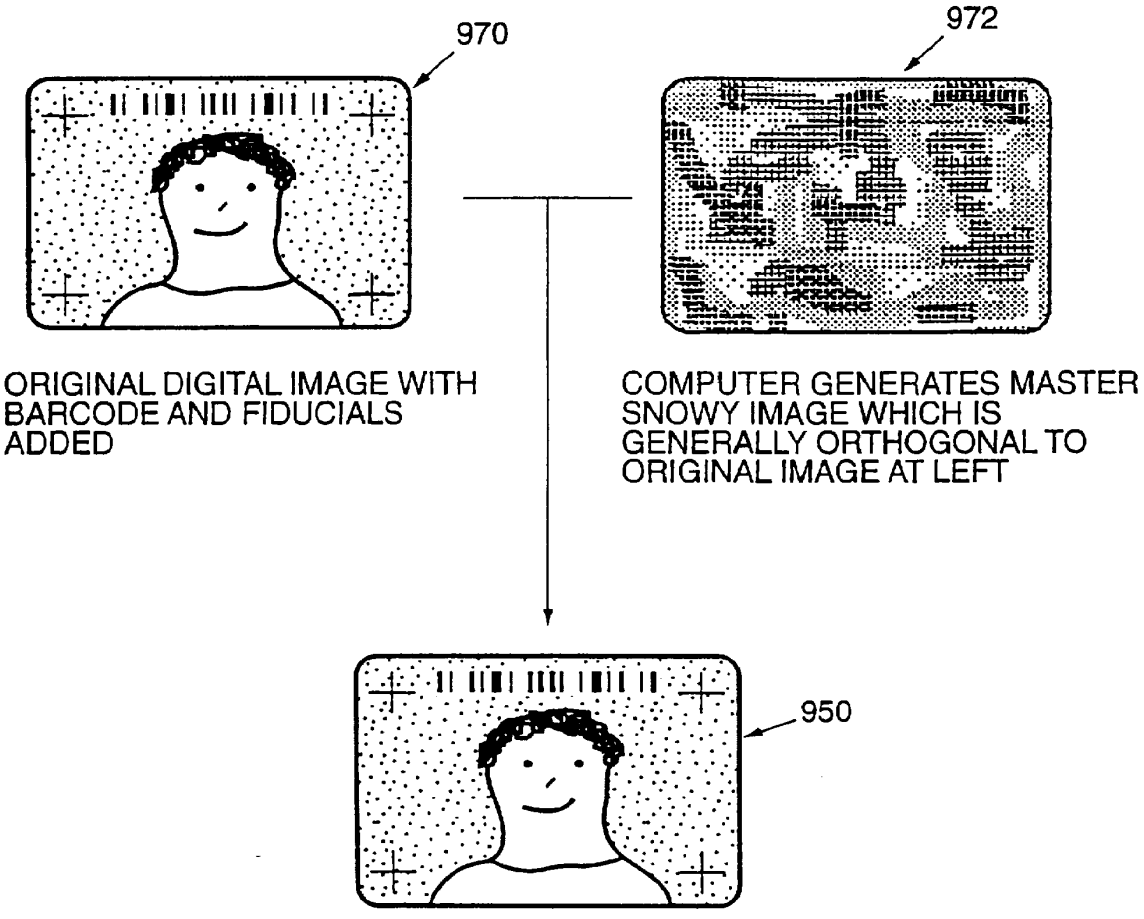

970
972
ORIGINAL DIGITAL IMAGE WITH BARCODE AND FIDUCIALS ADDED
COMPUTER GENERATES MASTER SNOWY IMAGE WHICH IS GENERALLY ORTHOGONAL TO ORIGINAL IMAGE AT LEFT
950
COMBINED TO FORM PERSONAL CASH CARD

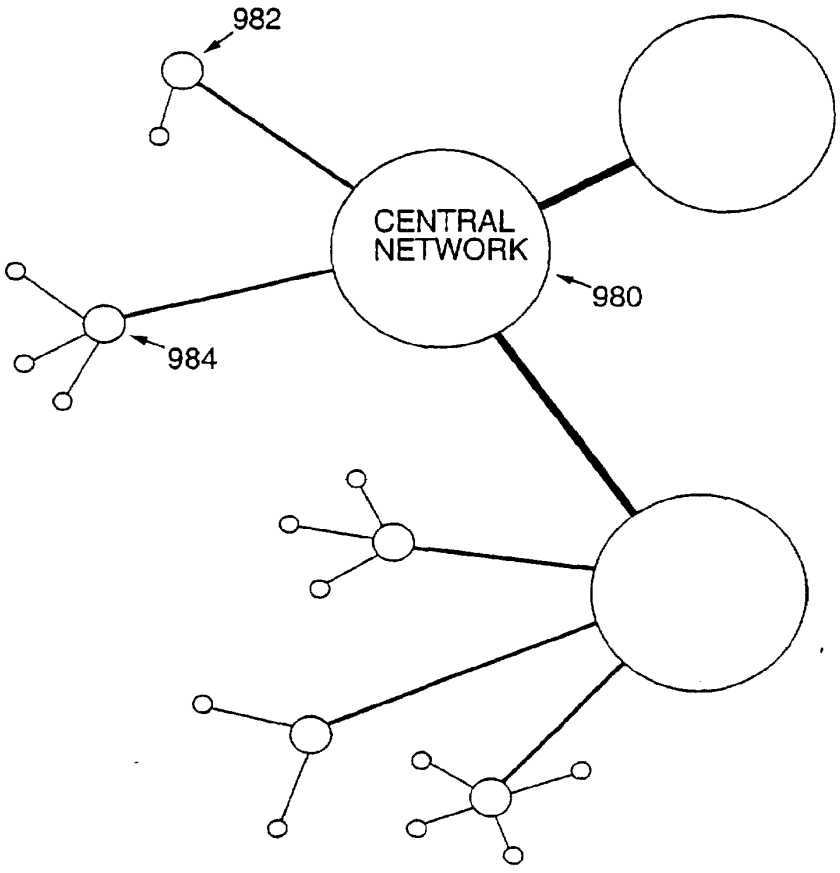
FIG. 25 TYPICAL TRANSACTION STEPS

1. READER SCANS IMAGE ON CARD, STORES IN MEMORY, EXTRACTS PERSON'S ID
2. OPTIONAL: USER KEYS IN PIN NUMBER
3. READER CALLS CENTRAL ACCOUNT DATA NETWORK, HANDSHAKES
4. READER SENDS ID, (PIN), MERCHANT INFORMATION, AND REQUESTED TRANSACTION AMOUNT TO CENTRAL NETWORK
5. CENTRAL NETWORK VERIFIES ID, PIN, MERCHANT INFO, AND ACCOUNT BALANCE
6. IF OK, CENTRAL NETWORK GENERATES TWENTY-FOUR SETS OF SIXTEEN DISTINCT RANDOM NUMBERS, WHERE THE RANDOM NUMBERS ARE INDEXES TO A SET OF 64K ORTHOGONAL SPATIAL PATTERNS
7. CENTRAL NETWORK TRANSMITS FIRST OK, AND THE SETS OF RANDOM NUMBERS
8. READER STEPS THROUGH THE TWENTY-FOUR SETS
   8A. READER ADDS TOGETHER SET OF ORTHOGONAL PATTERNS
   8B. READER PERFORMS DOT PRODUCT OF RESULTANT PATTERN AND CARD SCAN, STORES RESULT
9. READER TRANSMITS THE TWENTY-FOUR DOT PRODUCT RESULTS TO CENTRAL NETWORK
10. CENTRAL NETWORK CHECKS RESULTS AGAINST MASTER
11. CENTRAL NETWORK SENDS FINAL APPROVAL OR DENIAL
12. CENTRAL NETWORK DEBITS MERCHANT ACCOUNT, CREDITS CARD ACCOUNT

Ex.1002 / Page 633 of 1385
APPLE INC.

FIG. 26

THE NEGLIGIBLE-FRAUD CASH CARD SYSTEM



A BASIC FOUNDATION OF THE CASH CARD SYSTEM IS A 24-HOUR INFORMATION NETWORK, WHERE BOTH THE STATIONS WHICH CREATE THE PHYSICAL CASH CARDS, 950, AND THE POINT-OF-SALES, 984, ARE ALL HOOKED UP TO THE SAME NETWORK CONTINUOUSLY

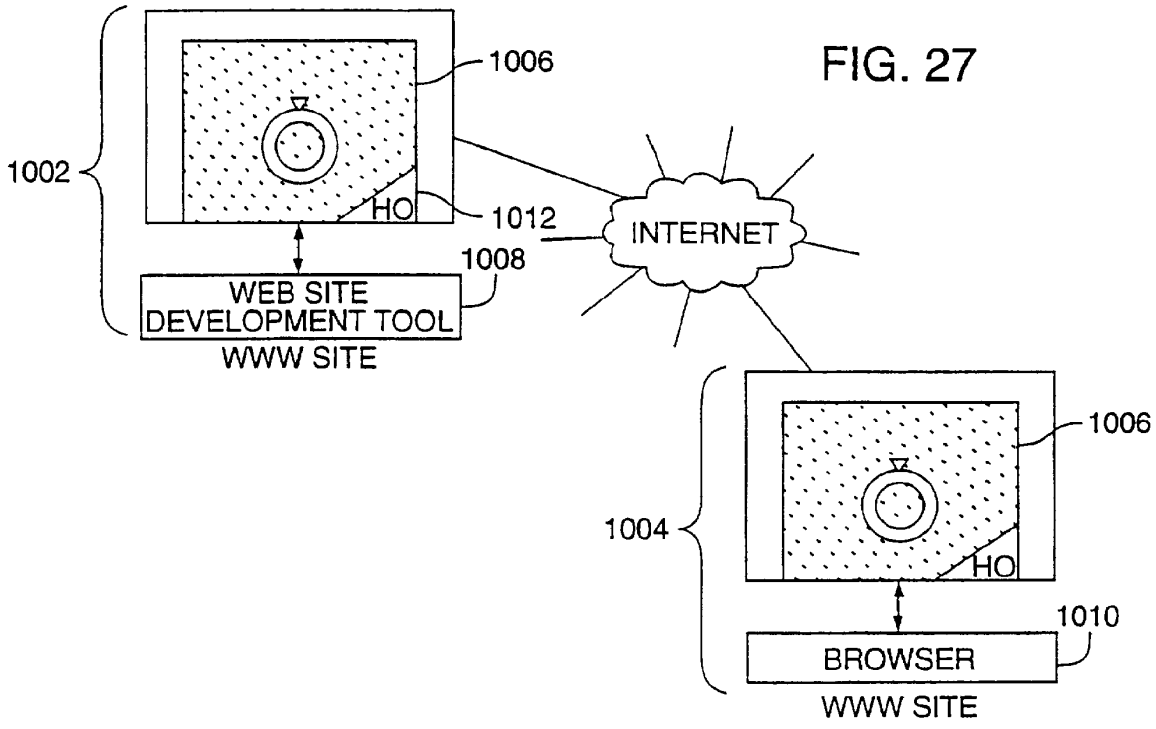

1002
1006
HO
1012
INTERNET
1008
WEB SITE
DEVELOPMENT TOOL
WWW SITE
1004
1006
HO
1010
BROWSER
WWW SITE

FIG. 27

FIG. 28

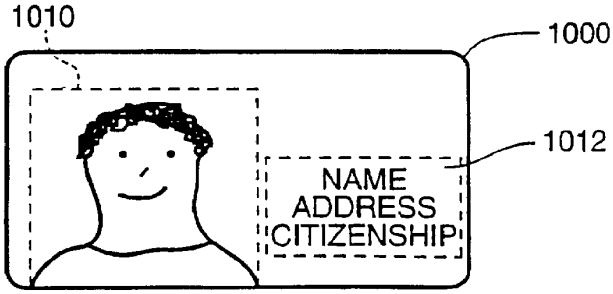

1010
1000
1012
NAME
ADDRESS
CITIZENSHIP

FIG. 27A

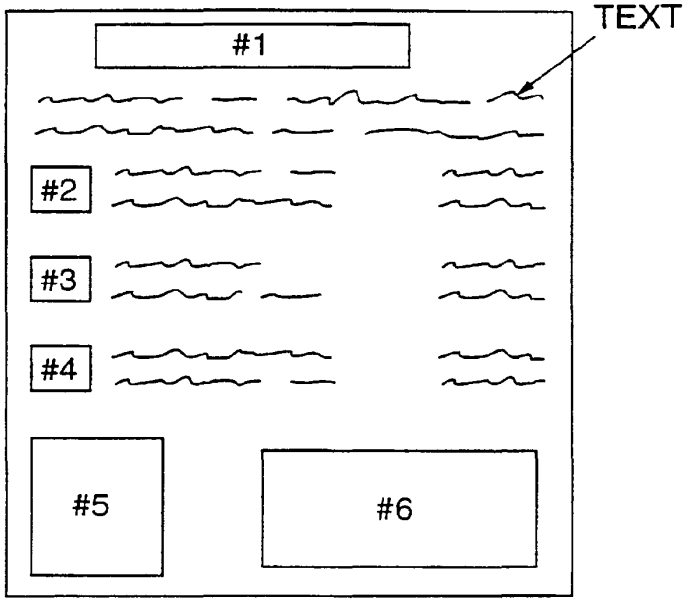


FIG. 27B

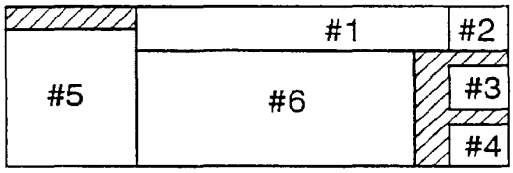
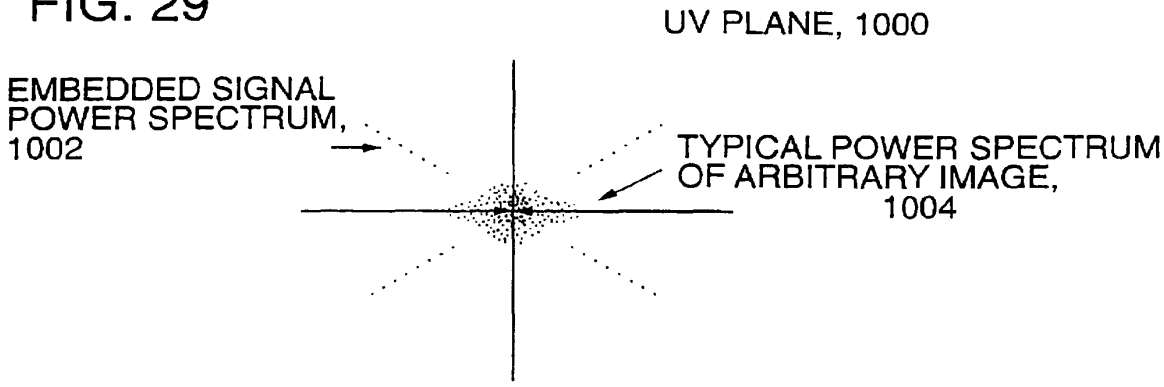
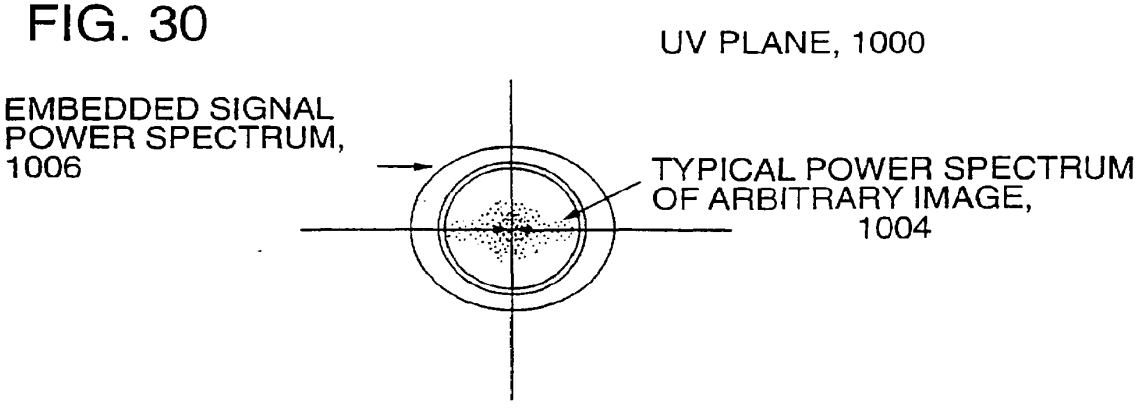


FIG. 29



NON-HARMONIC SPATIAL FREQUENCIES ALONG THE 45 DEGREE AXES, GIVING RISE TO A WEAVE-LIKE CROSS-HATCHING PATTERN IN THE SPATIAL DOMAIN

FIG. 30



NON-HARMONIC CONCENTRIC CIRCLES IN UV PLANE, WHERE PHASE HOPS QUASI-RANDOMLY ALONG EACH CIRCLE, GIVING RISE TO PSEUDO RANDOM LOOKING PATTERNS IN THE SPATIAL DOMAIN

FIG. 29A

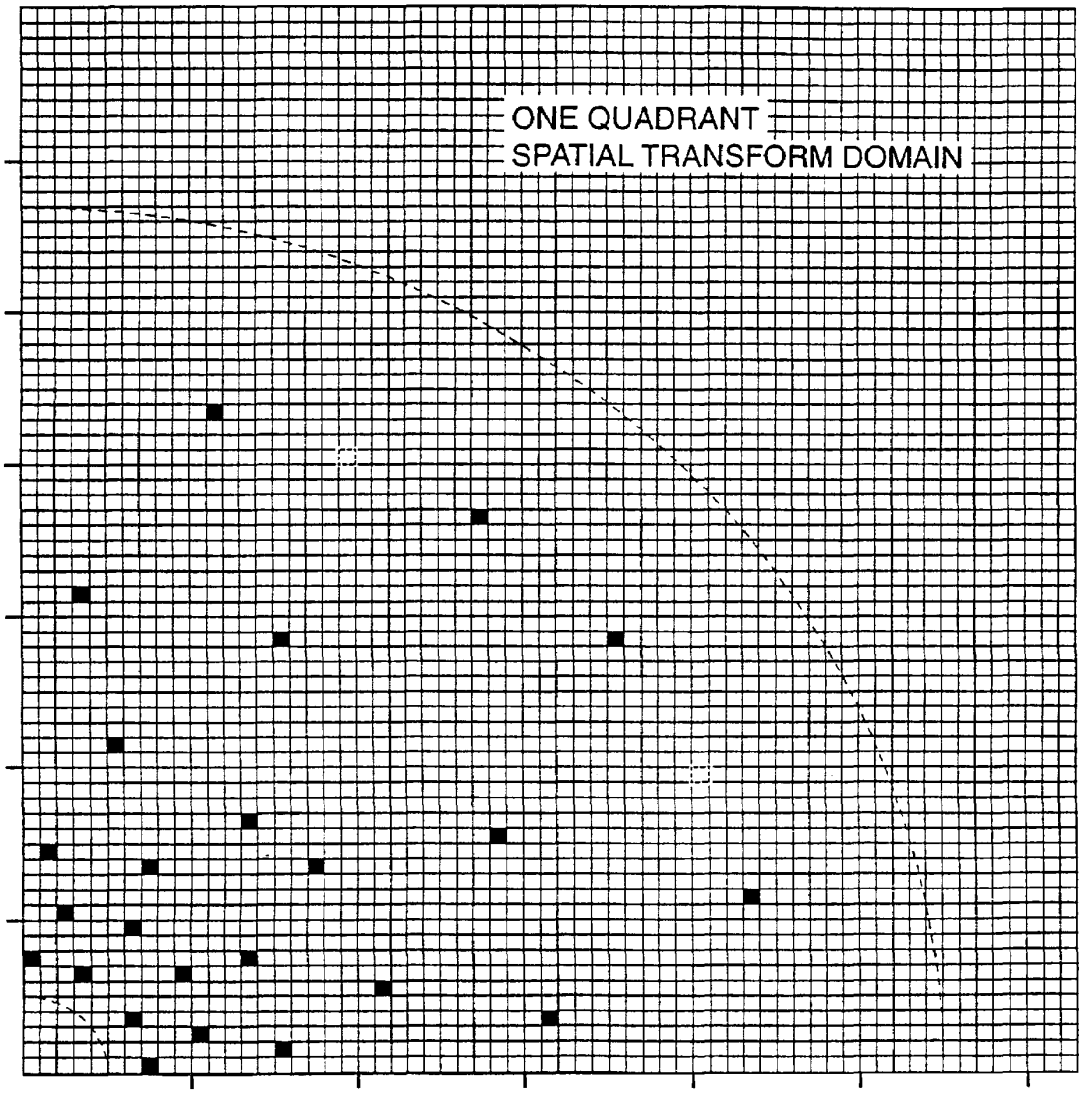
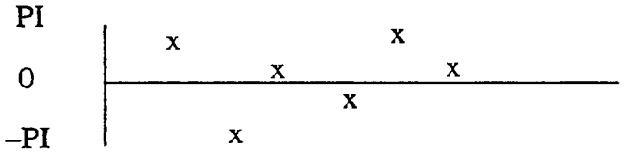
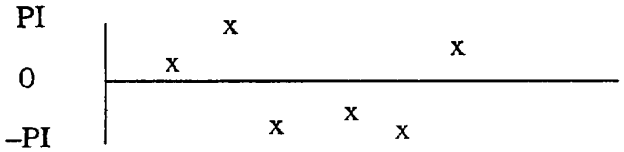


FIG. 31A



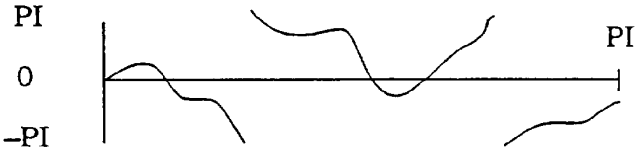
PHASE OF SPATIAL FREQUENCIES ALONG FORWARD 45 DEGREE AXES, 1008

FIG. 31B



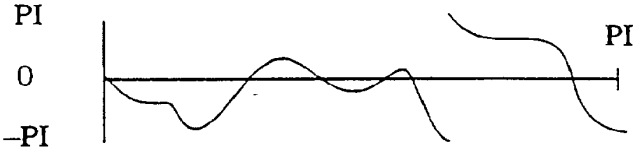
PHASE OF SPATIAL FREQUENCIES ALONG BACKWARD 45 DEGREE AXES, 1010

FIG. 32A



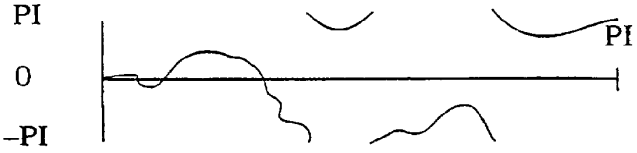
PHASE OF SPATIAL FREQUENCIES ALONG FIRST CONCENTRIC RING, 1012

FIG. 32B



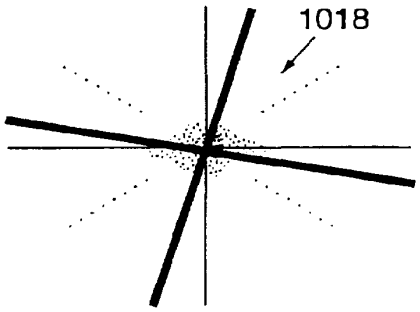
PHASE OF SPATIAL FREQUENCIES ALONG SECOND CONCENTRIC RING, 1014

FIG. 32C



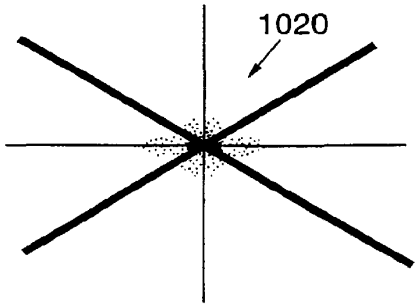
PHASE OF SPATIAL FREQUENCIES ALONG THIRD CONCENTRIC RING, 1016

FIG. 33A



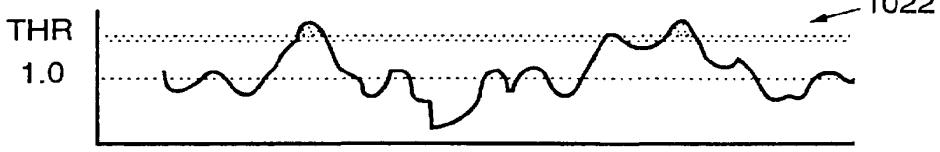
ANGLE A

FIG. 33B



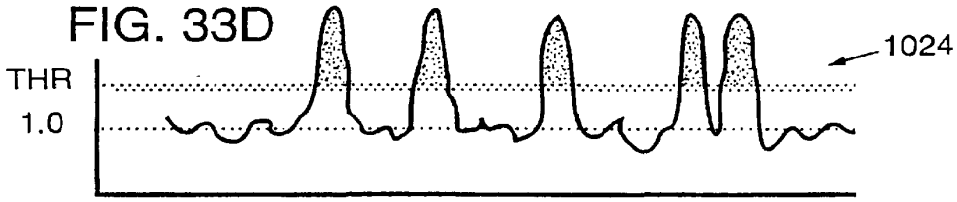
ANGLE B

FIG. 33C



POWER PROFILE ALONG ANGLE A, AS NORMALIZED BY ITS OWN MOVING AVERAGE; ONLY A MINIMAL AMOUNT EXCEEDS THRESHOLD, GIVING A SMALL INTEGRATED VALUE

FIG. 33D



POWER PROFILE ALONG ANGLE B, AS NORMALIZED BY ITS OWN MOVING AVERAGE; THIS FINDS STRONG ENERGY ABOVE THE THRESHOLD

FIG. 33E

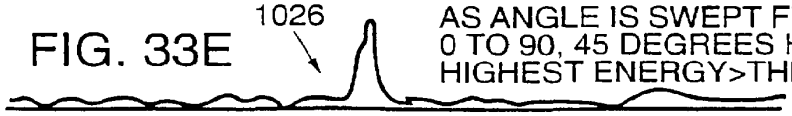


FIG. 34A

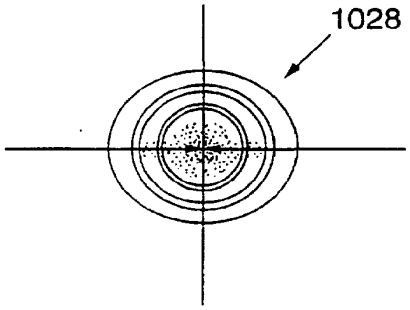


FIG. 34B

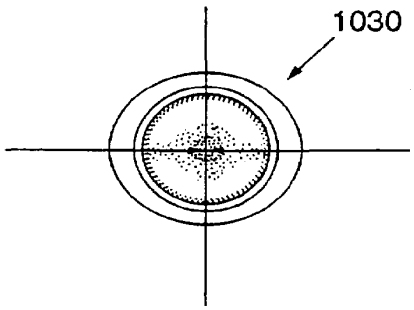
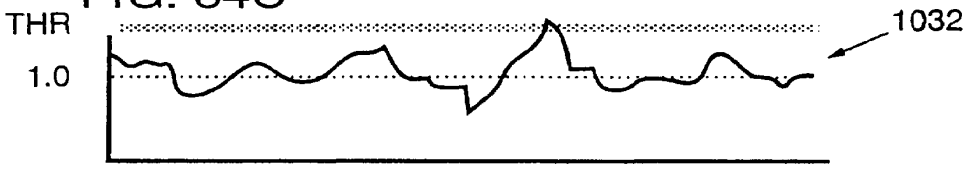
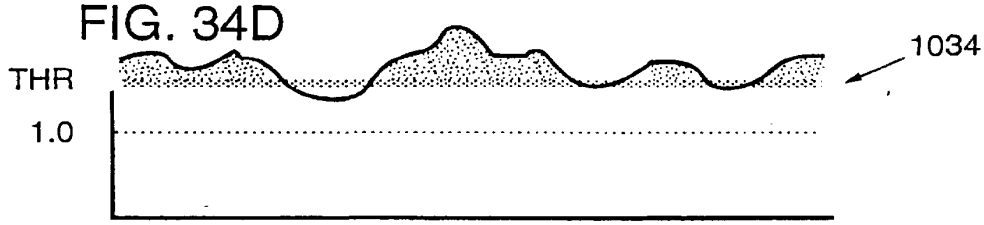


FIG. 34C



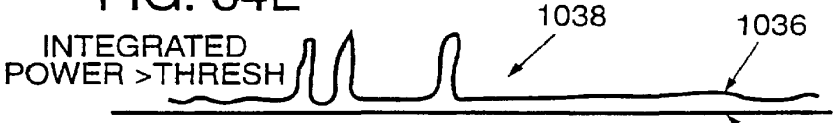
POWER PROFILE ALONG CIRCLE AT RADIUS A

FIG. 34D



POWER PROFILE ALONG CIRCLE AT RADIUS B

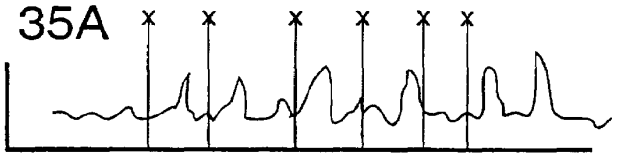
FIG. 34E



TOTAL INTEGRATED POWER ABOVE THRESHOLD AS FUNCTION OF RADIUS

1040

FIG. 35A



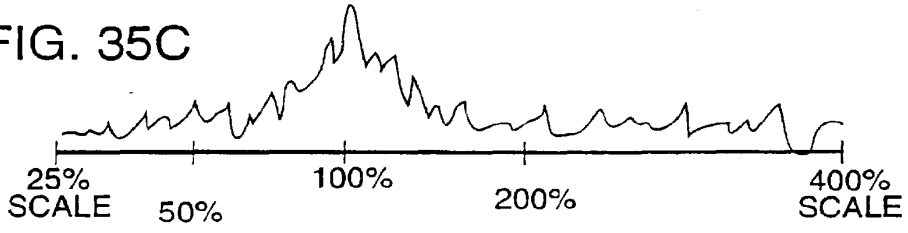
SCALE = A; ADD ALL POWER VALUES AT THE "KNOWN" FREQUENCIES", 1042

FIG. 35B



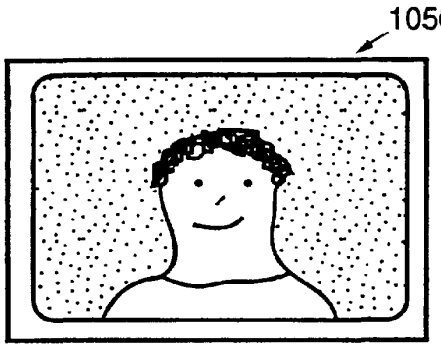
SCALE = B; ADD ALL POWER VALUES AT THE "KNOWN" FREQUENCIES", 1044

FIG. 35C



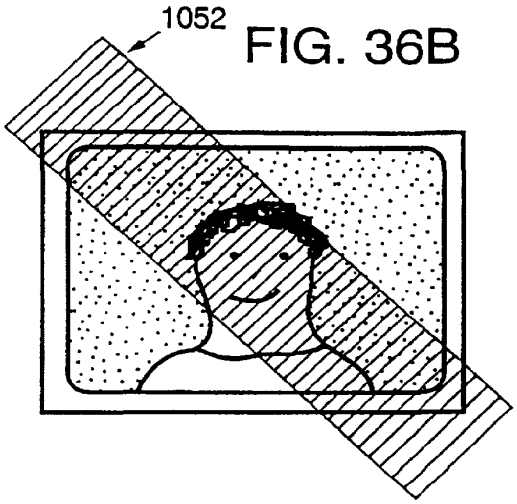
"SCALED-KERNEL" BASED MATCHED FILTER; PEAK IS WHERE THE SCALE OF THE SUBLIMINAL GRID WAS FOUND, 1046

FIG. 36A



ARBITRARY ORIGINAL IMAGE
IN WHICH SUBLIMINAL
GRATICULES MAY HAVE BEEN PLACED

FIG. 36B



"COLUMN SCAN"
IS APPLIED ALONG A
GIVEN ANGLE THROUGH
THE CENTER OF THE
IMAGE

FIG. 36C

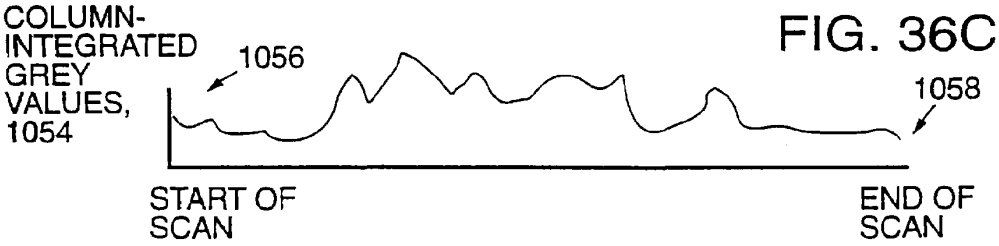
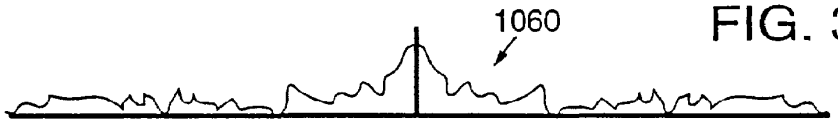


FIG. 36D



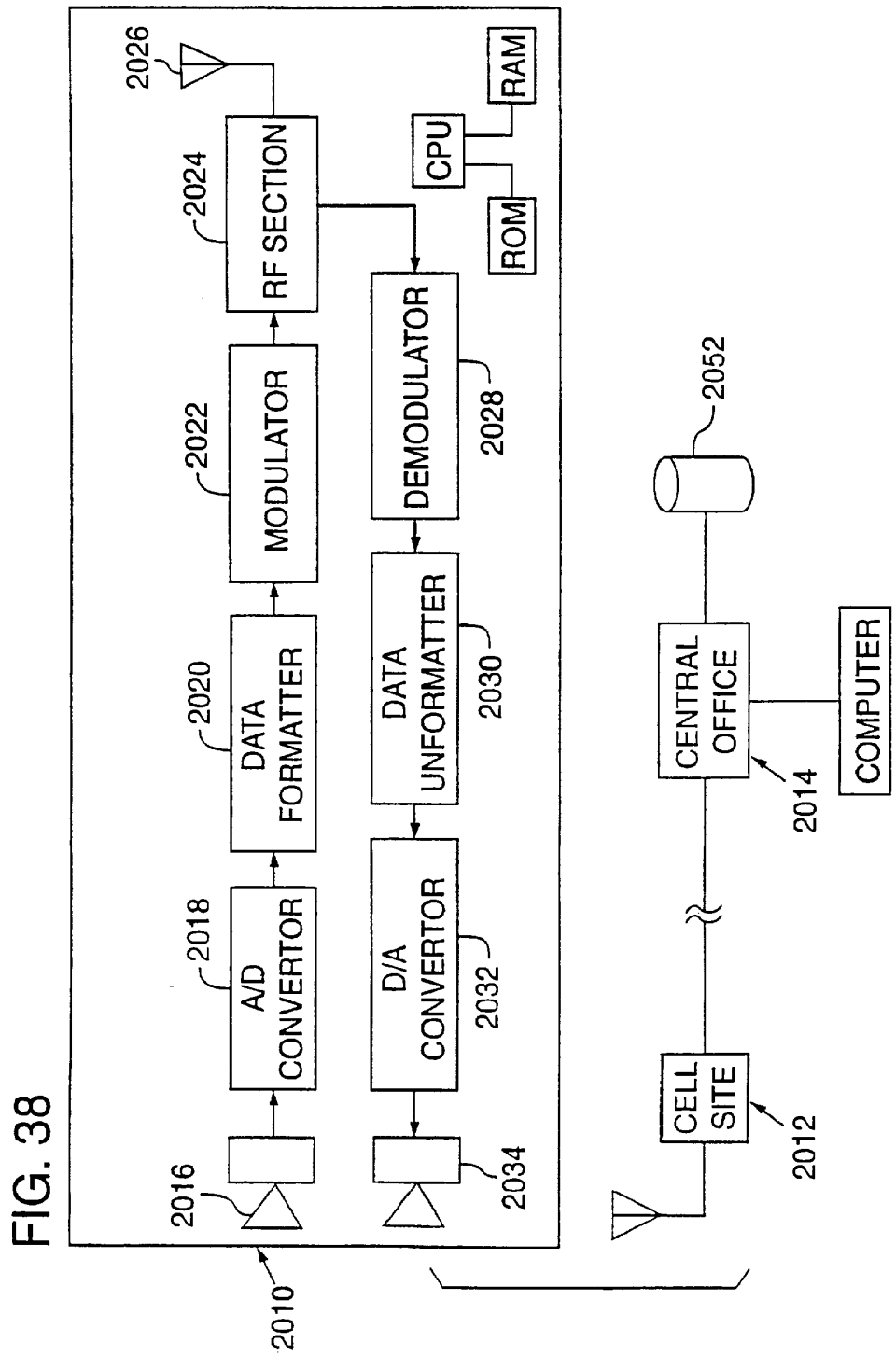
MAGNITUDE OF FOURIER TRANSFORM OF SCAN DATA

FIG. 37

PROCESS STEPS

1. SCAN IN PHOTOGRAPH
2. 2D FFT
3. GENERATE 2D POWER SPECTRUM, FILTER WITH E.G. 3X3 BLURRING KERNEL
4. STEP ANGLES FROM 0 DEGREES THROUGH 90 (1/2 DEG)
5. GENERATE NORMALIZED VECTOR, WITH POWER VALUE AS NUMERATOR, AND MOVING AVERAGED POWER VALUE AS DENOMINATOR
6. INTEGRATE VALUES AS SOME THRESHOLD, GIVING A SINGLE INTEGRATED VALUE FOR THIS ANGLE
7. END STEP ON ANGLES
8. FIND TOP ONE OR TWO OR THREE "PEAKS" FROM THE ANGLES IN LOOP 4, THEN FOR EACH PEAK...
9. STEP SCALE FROM 25% TO 400%, STEP ~1.01
10. ADD THE NORMALIZED POWER VALUES CORRESPONDING TO THE 'N' SCALED FREQUENCIES OF STANDARD
11. KEEP TRACK OF HIGHEST VALUE IN LOOP
12. END LOOP 9 AND 8, DETERMINE HIGHEST VALUE
13. ROTATION AND SCALE NOW FOUND
14. PERFORM TRADITIONAL MATCHED FILTER TO FIND EXACT SPATIAL OFFSET
15. PERFORM ANY "FINE TUNING" TO PRECISELY DETERMINE ROTATION, SCALE, OFFSET

FIG. 38


2010
2012
2014
2016
2018
2020
2022
2024
2026
2028
2030
2032
2034
2052
A/D CONVERTOR
DATA FORMATTER
MODULATOR
RF SECTION
D/A CONVERTOR
DATA UNFORMATTER
DEMODULATOR
CPU
RAM
ROM
CELL SITE
CENTRAL OFFICE
COMPUTER

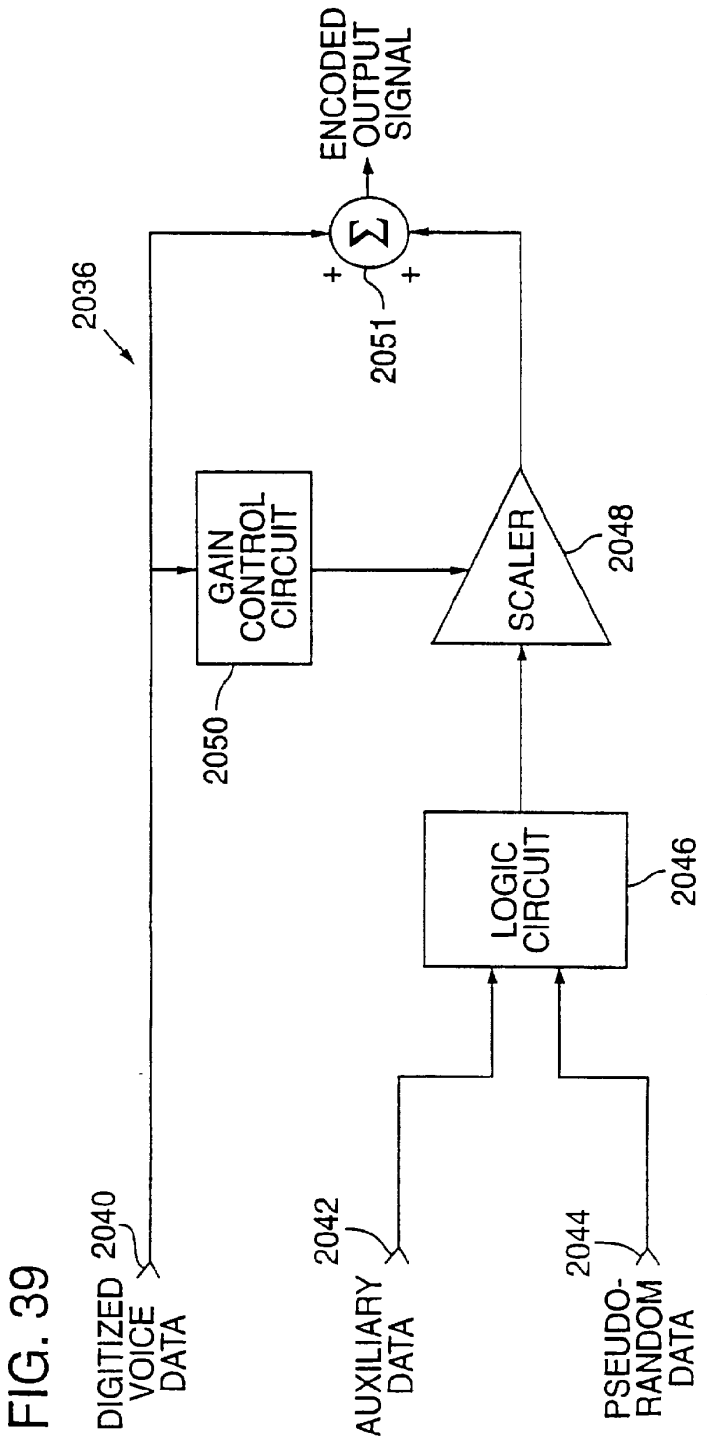

ENCODED OUTPUT SIGNAL
Σ
+
+
2051
2036
GAIN CONTROL CIRCUIT
2050
SCALER
2048
LOGIC CIRCUIT
2046
DIGITIZED VOICE DATA
2040
AUXILIARY DATA
2042
PSEUDO-RANDOM DATA
2044

FIG. 39

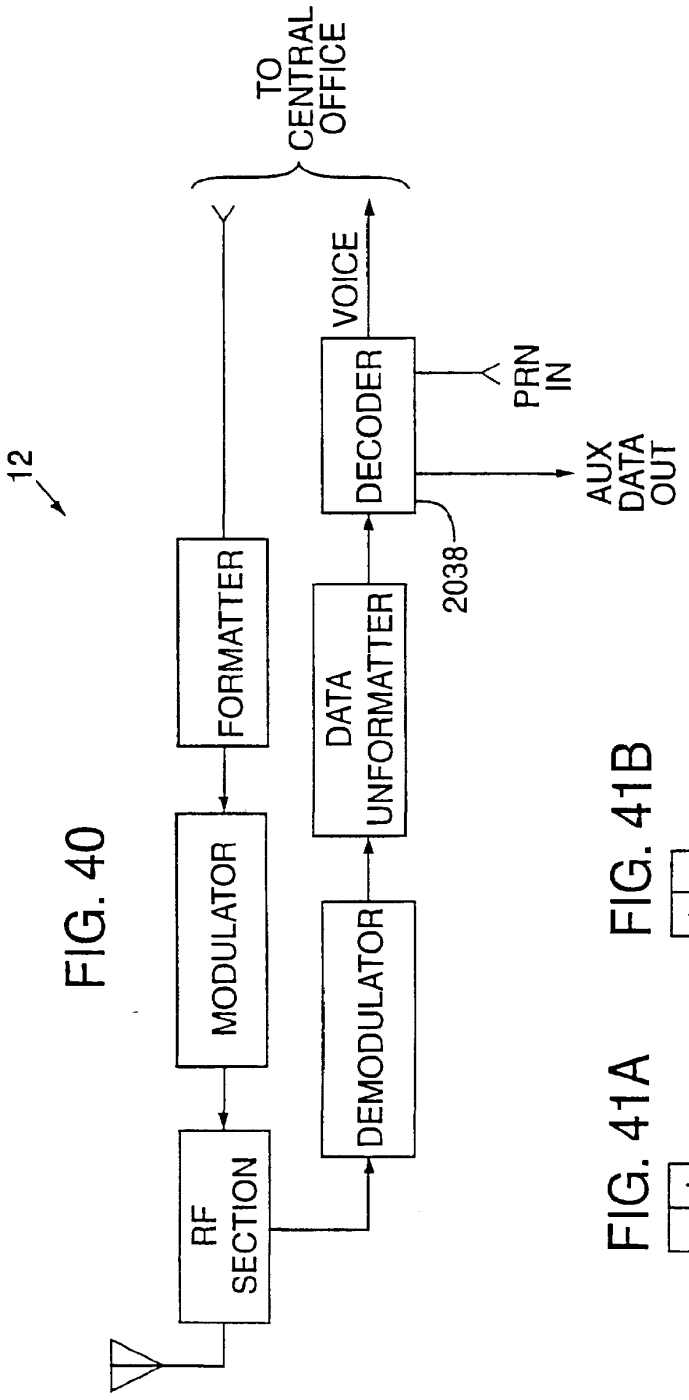


FIG. 40

FIG. 41A

−	+
+	−

FIG. 41B

−	+
+	−

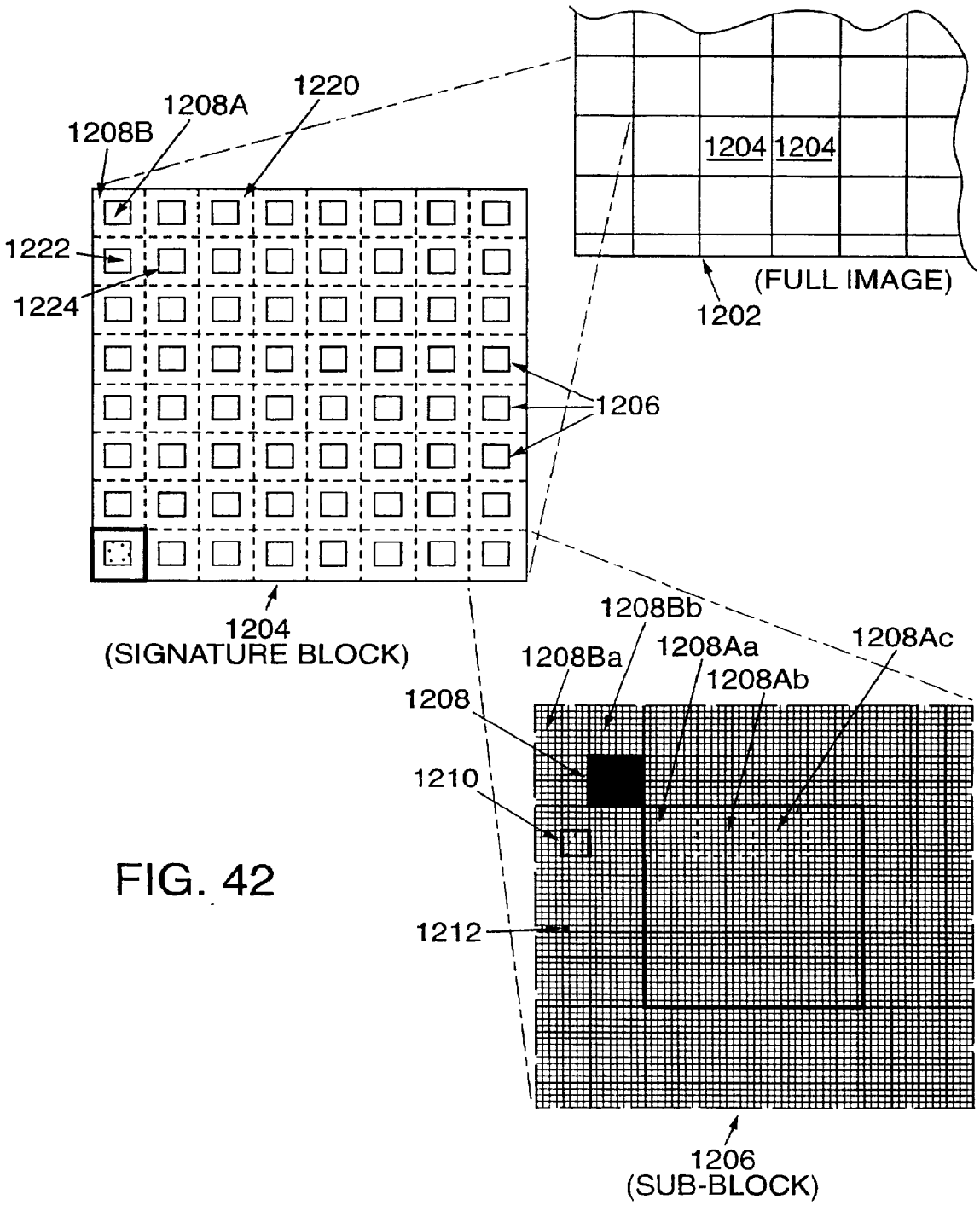

1220
1208A
1208B
1222
1224
1204 1204
(FULL IMAGE)
1202
1206
1204
(SIGNATURE BLOCK)
1208Bb
1208Ba
1208Aa
1208Ac
1208Ab
1208
1210
1212
1206
(SUB-BLOCK)

FIG. 42

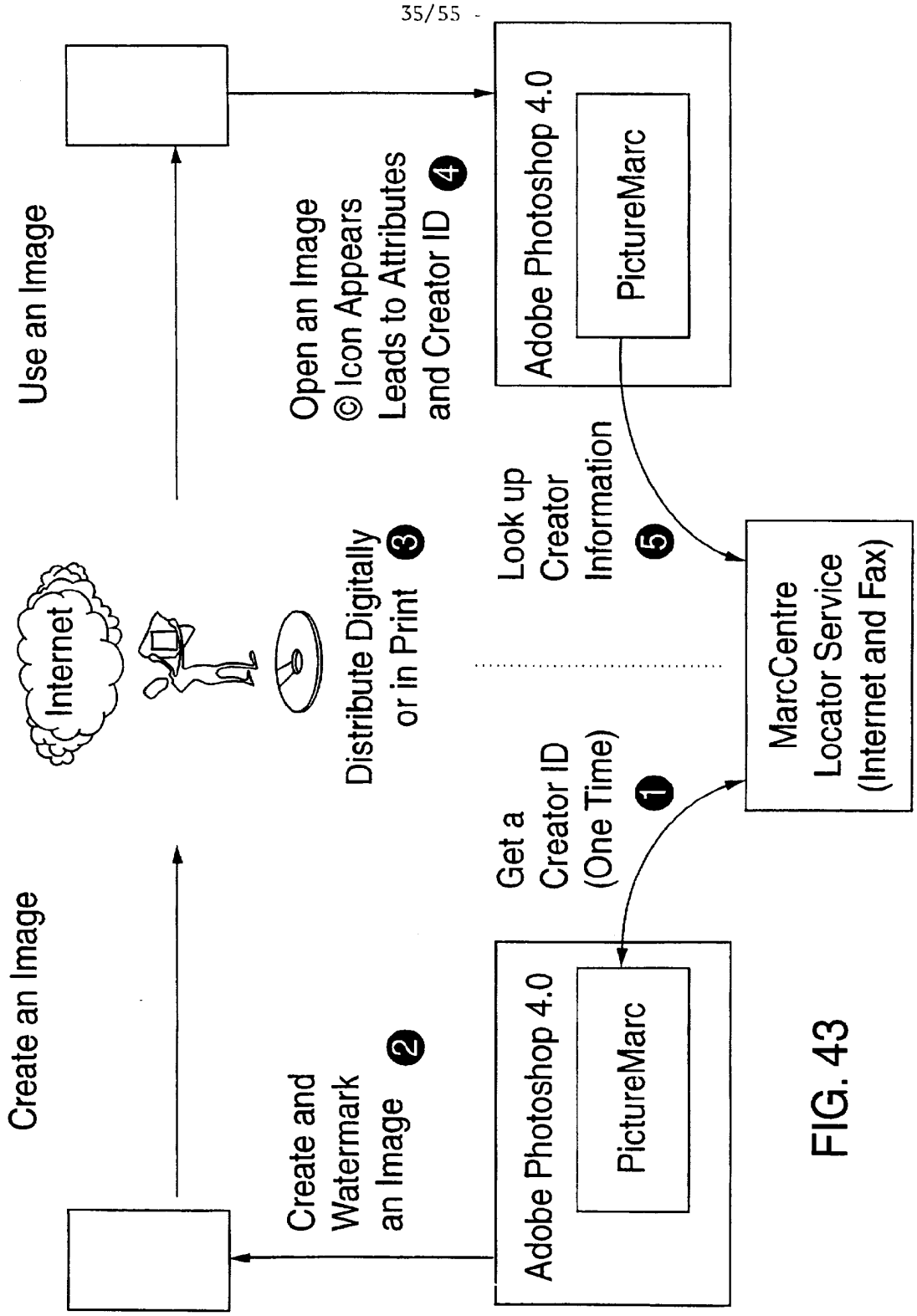

Create an Image
Create and Watermark an Image 2
Adobe Photoshop 4.0
PictureMarc
Get a Creator ID (One Time) 1
MarcCentre Locator Service (Internet and Fax)
Look up Creator Information 5
Distribute Digitally or in Print 3
Internet
Open an Image © Icon Appears Leads to Attributes and Creator ID 4
Adobe Photoshop 4.0
PictureMarc
Use an Image

FIG. 43

MarcCentre file:///C|/Data/Downlo



Welcome to MarcCentre™ Digimarc's Locator Service

MarcCentre is an on-line service which links your up-to-date contact information to every image you watermark. You provide the details you want consumers of your image to see. Each time someone reads one of your watermarked images, they can access this information about you and your work with a single mouse click.

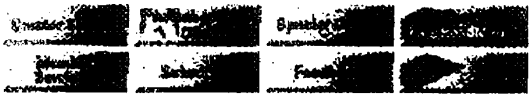
Subscribe now to give each of your images a persistent identity, communicating your copyright, and bringing consumers directly to you. Take advantage of the special offers available to you now, for a limited time.

To find out more about how MarcCentre works and how you can get started taking advantage of this locator service, browse the MarcCentre overview page.

If you are already a subscriber, you can go to Member Services to view or update your contact details.

To look up image creator/distributor information, you can search by creator ID or by other, more general, criteria.

For the technically minded, find out what's going on behind the scenes.



Digimarc Copyright Notice | About the Site

FIG. 44

Subscription : Page 1

MarcCentre™ Digimarc Corporation

Thank you for signing up with MarcCentre. There are two parts to the application form (1) your contact information and (2) Agencies or Representative contact information. Simply fill in the blanks on this page and click "Part 1 Complete" below.

Name (First/Last)*
Company
Address*
City*
State/Province*
Zip/Postal Code*
Country*
Phone Number*
Fax Number
Email Address
Your Home Page http://

You can control how much of your contact information is displayed when a potential customer finds your profile on MarcCentre. Use the selections below to tell us what you want people to see.

Phone Number	Mailing Address	Email Account
(•) Show	(•) Show	(•) Show
( ) Don't show	( ) Don't show	( ) Don't show

Yes, I want to be on your mailing lists [X]

Please select your profession (one only).

(•) Photographer
( ) Illustrator
( ) Other

In order to communicate your primary area of focus or specialty to potential customers, please select one of the options from the list below -or- type in your own in the space next to "Custom Specialty"

Photographer: (none)
Illustrator: (none)
Custom Specialty

FIG. 45

Subscription : Page 2 of 2

Digimarc displays an Image of the Day showcase on our web site. Would you like to participate?
◉ Yes.
○ Not at this time.
For security purposes, you will need to setup a password that allows you to edit your profile information. This password along with your Creator ID are required before you can update your contact information.

Password* Re-enter to verify*

The standard fee for the MarcCentre service is $150 (US). From now until December 31st, 1995 you can subscribe for only $79 (US), over 50% off the regular price!
For security reasons, the following credit card information is captured using secure Digimarc displays an Image of the Day showcase on our web site. Would
Credit you like to participate?
◉ Visa ◉ Yes.
○ MasterCard
○ American Express

Card Number* Name Shown on Card* Expiration (MM/YY)*

When you are satisfied with your entries on this form press the "Part 1 Complete" button and continue with the second part of the subscription sign-up. If you wish to cancel, press the Back button on your browser.

Part 1 Complete

Digimarc Copyright Notice

FIG. 46

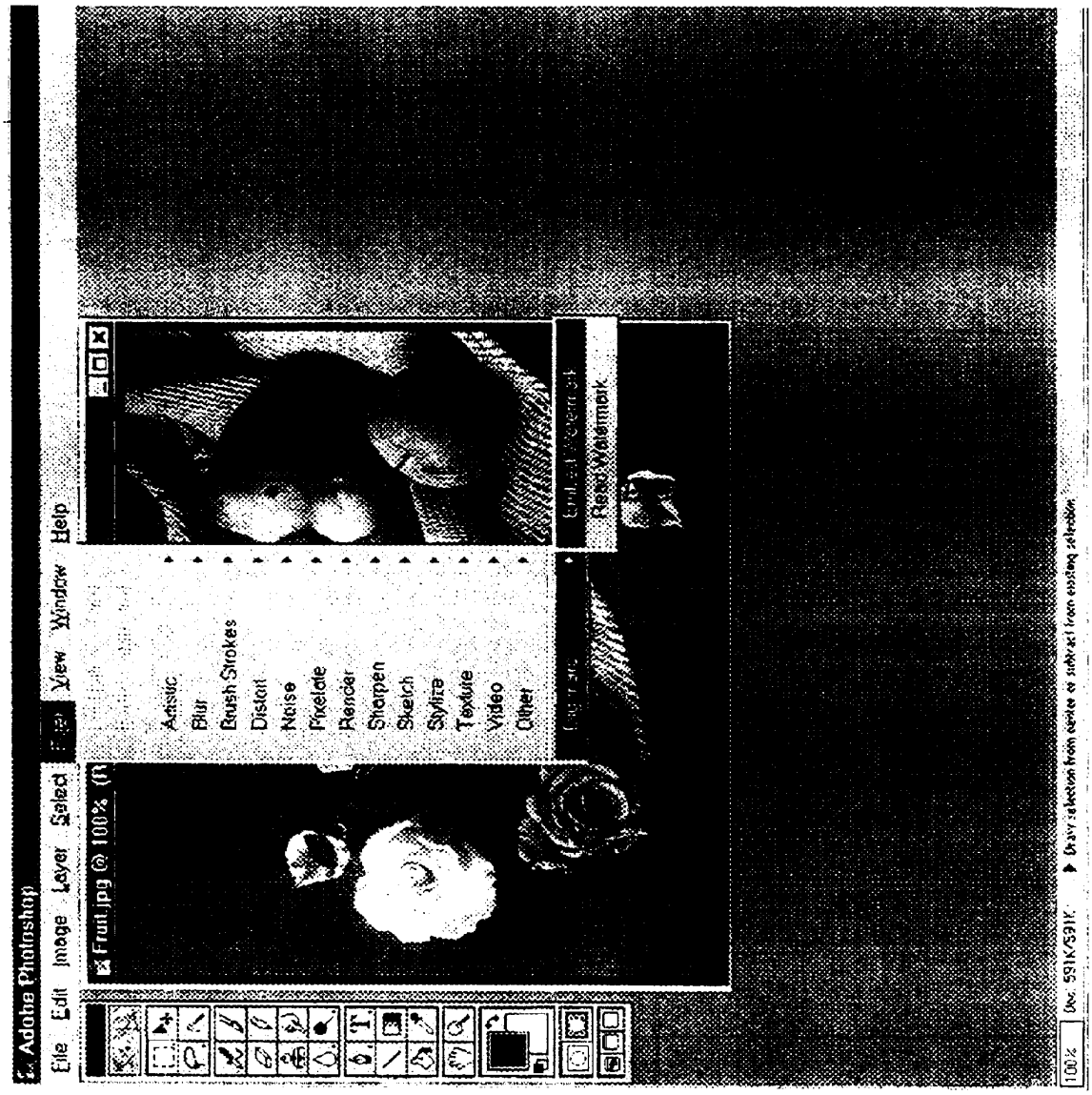

Adobe Photoshop
File Edit Image Layer Select View Window Help
Artistic
Blur
Brush Strokes
Distort
Noise
Pixelate
Render
Sharpen
Sketch
Stylize
Texture
Video
Other
Embed Watermark
Read Watermark

FIG. 47


File Edit Image Layer Select Filter View Window Help
Copyright Info
Creator ID PictureMarc Demo
Personalize
Type of Use
Restricted
Royalty Free
Adult Content
OK
Cancel
Watermark Durability
less visible
more visible
less durable
more durable

FIG. 48

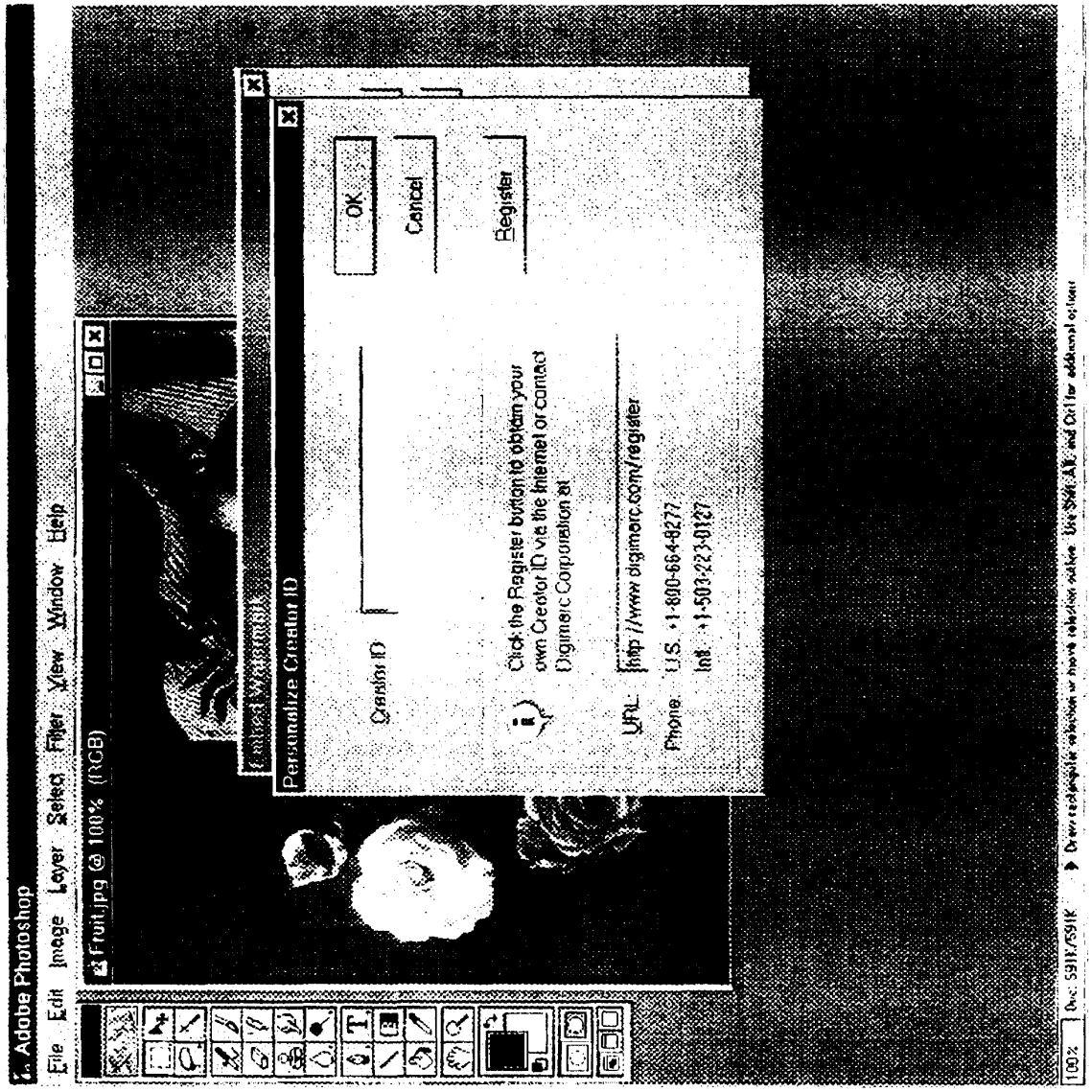

Adobe Photoshop
File Edit Image Layer Select Filter View Window Help
Fruit.jpg @ 100% (RGB)
Embed Watermark
Personalize Creator ID
Creator ID
OK
Cancel
Register
Click the Register button to obtain your own Creator ID via the Internet or contact Digimarc Corporation at
URL: http://www.digimarc.com/register
Phone: U.S. +1-800-664-8277
Int'l +1-503-223-0127

FIG. 49

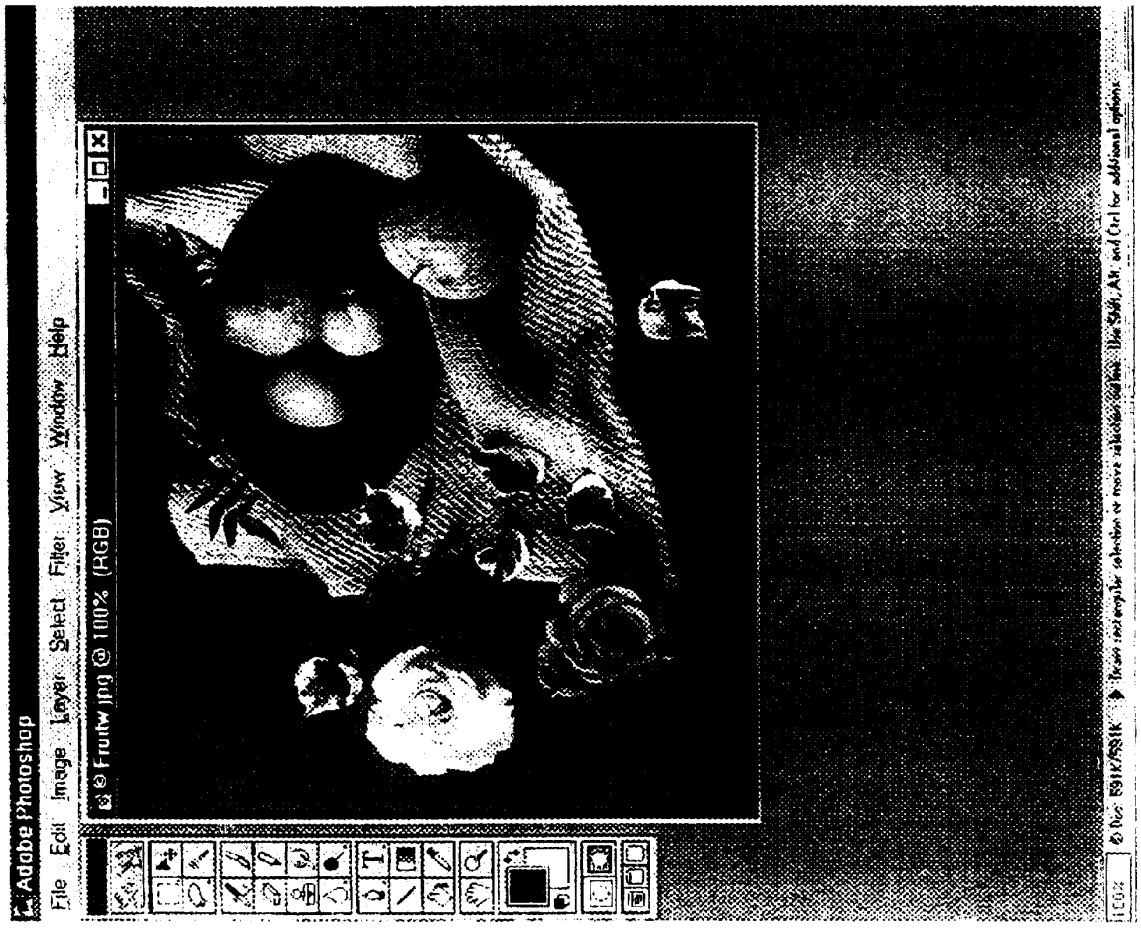

Adobe Photoshop
File Edit Image Layer Select Filter View Window Help
Fruitw.jpg @ 100% (RGB)

FIG. 50

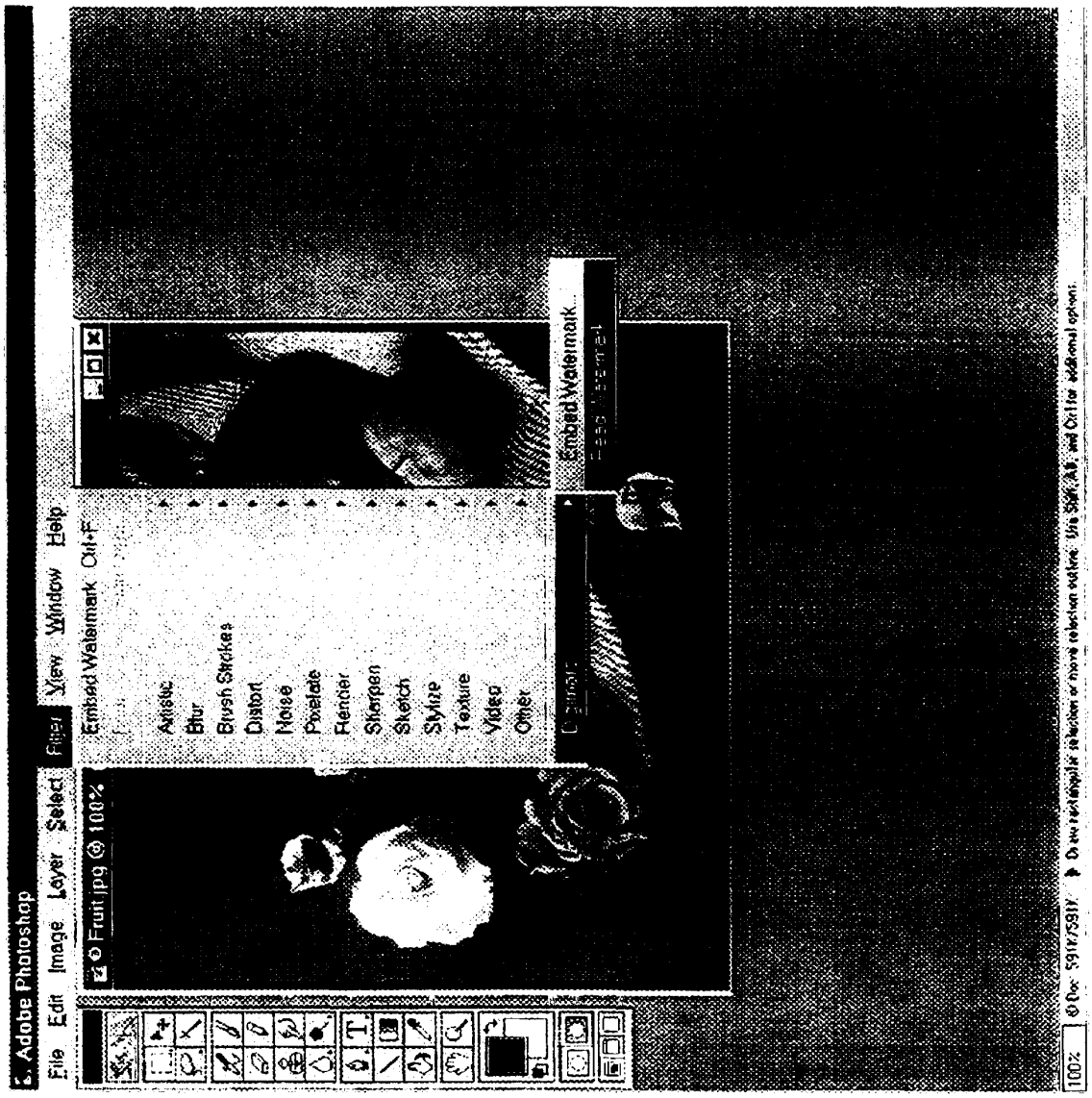

Adobe Photoshop
File Edit Image Layer Select Filter View Window Help
Embed Watermark Ctrl+F
Artistic
Blur
Brush Strokes
Distort
Noise
Pixelate
Render
Sharpen
Sketch
Stylize
Texture
Video
Other
Fruit.jpg @ 100%
Embed Watermark...
100%

FIG. 51

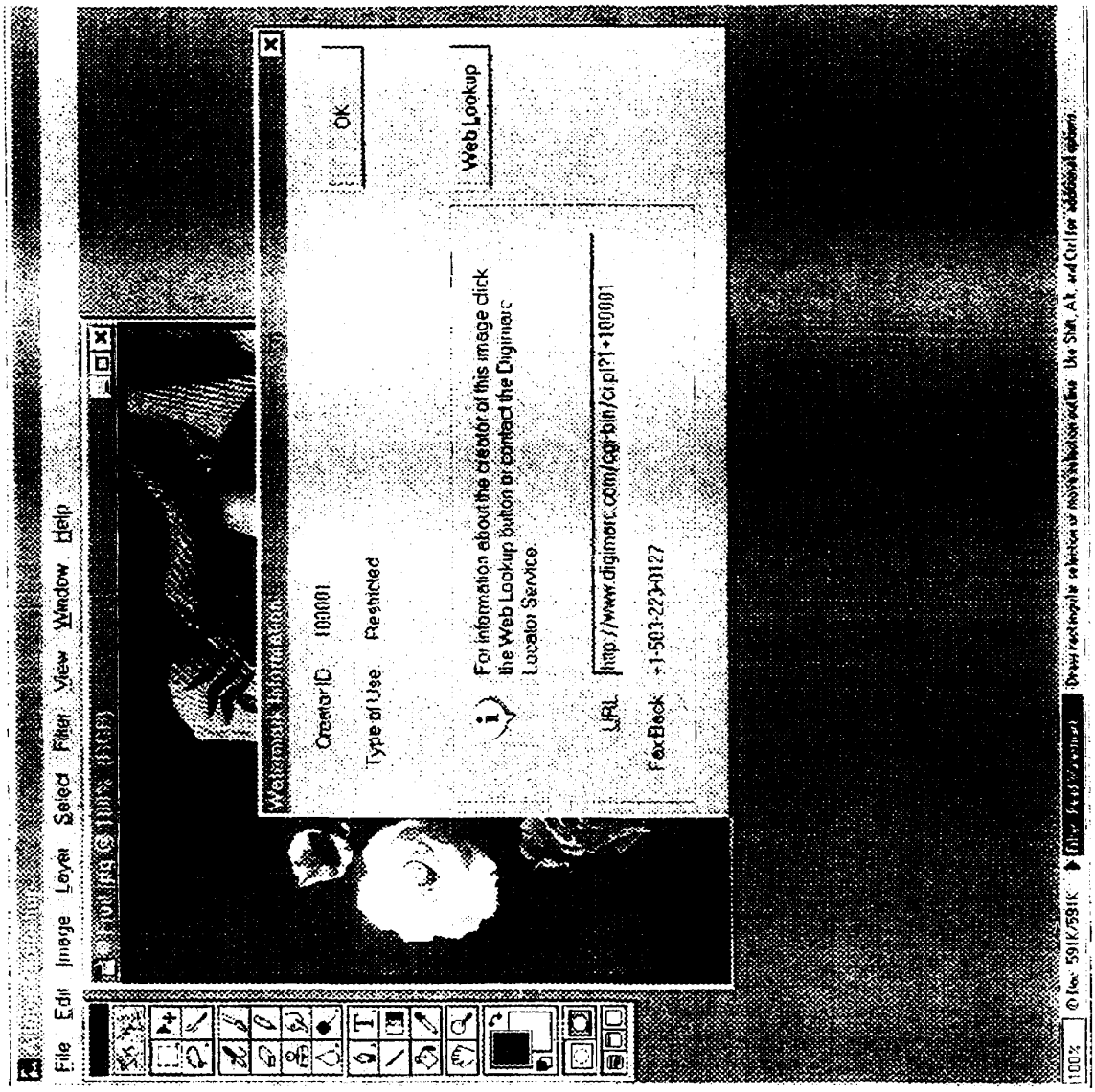

File Edit Image Layer Select Filter View Window Help
Watermark Information
Creator ID 100001
Type of Use Restricted
OK
For information about the creator of this image click the Web Lookup button or contact the Digimarc Locator Service.
Web Lookup
URL http://www.digimarc.com/cgi-bin/ci.pl?1+100001
Fax Back +1-503-223-0127

FIG. 52

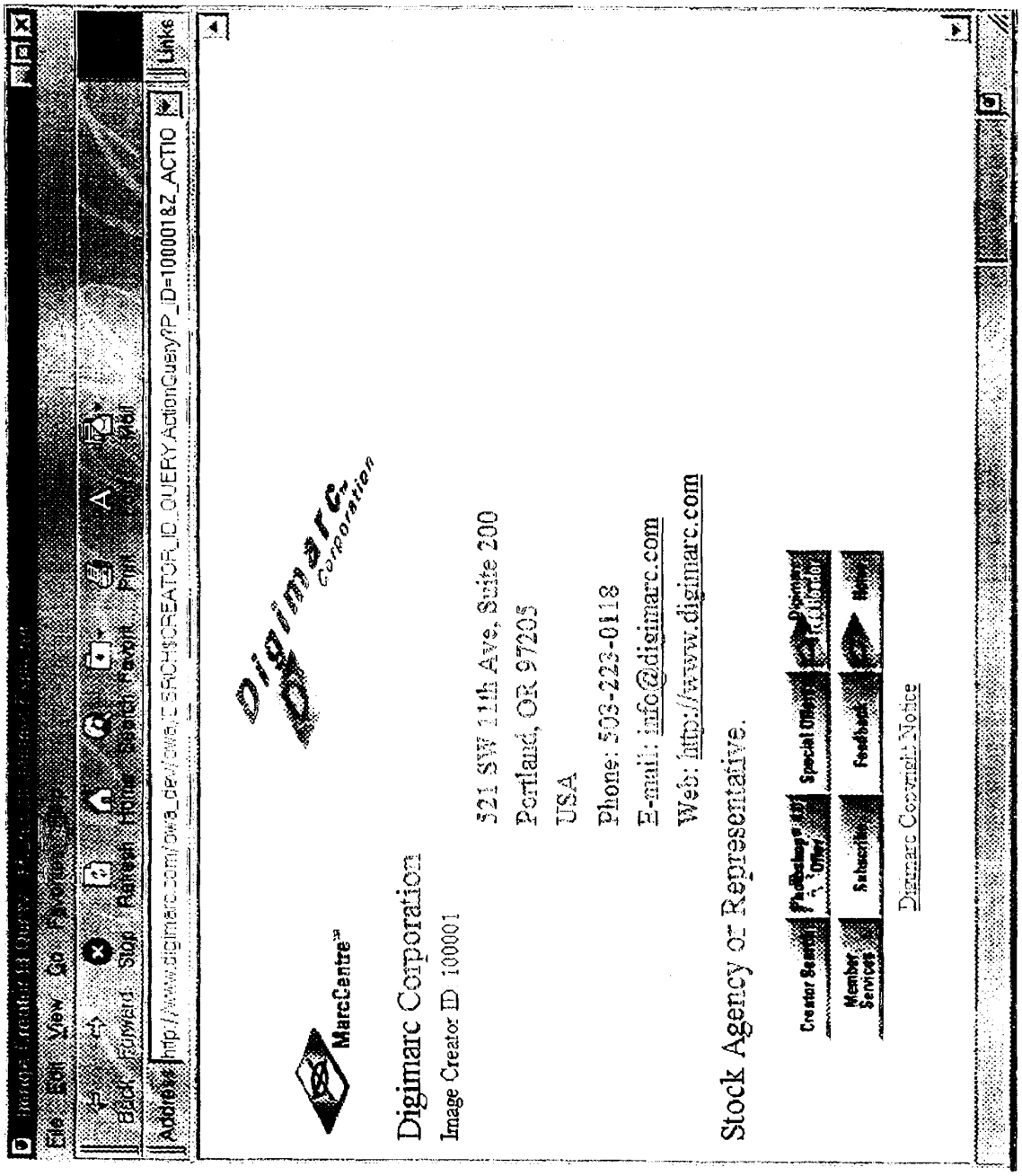

File Edit View Go
Back Forward Stop Refresh Home Search Favorit Print
Address http://www.digimarc.com/cgi-bin/DWEB_SRCH$CREATOR_ID_QUERY.ActionQuery?P_ID=100001&Z_ACTIO
Links
MarcCentre™
Digimarc Corporation
Digimarc Corporation
Image Creator ID 100001
521 SW 11th Ave, Suite 200
Portland, OR 97205
USA
Phone: 503-223-0118
E-mail: info@digimarc.com
Web: http://www.digimarc.com
Stock Agency or Representative.
Creator Services
Special Offers
Member Services
Subscription
Feedback
Digimarc Copyright Notice

FIG 53

Subscription : Page 1 of 1





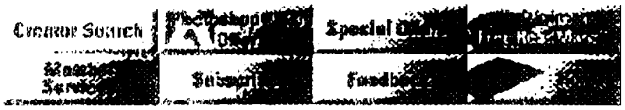
MarcCentre Image Creator Search

Enter the Image Creator ID in the box below and press "Submit Search". If it is a valid ID, the contact information details will be listed.

Image Creator ID: [ ] Submit Search

If you want to search for specific image creators by a variety of criteria such as last name, specialty, city and/or state then press the "General Search" button below.

General Search



Digimarc Copyright Notice

FIG. 54

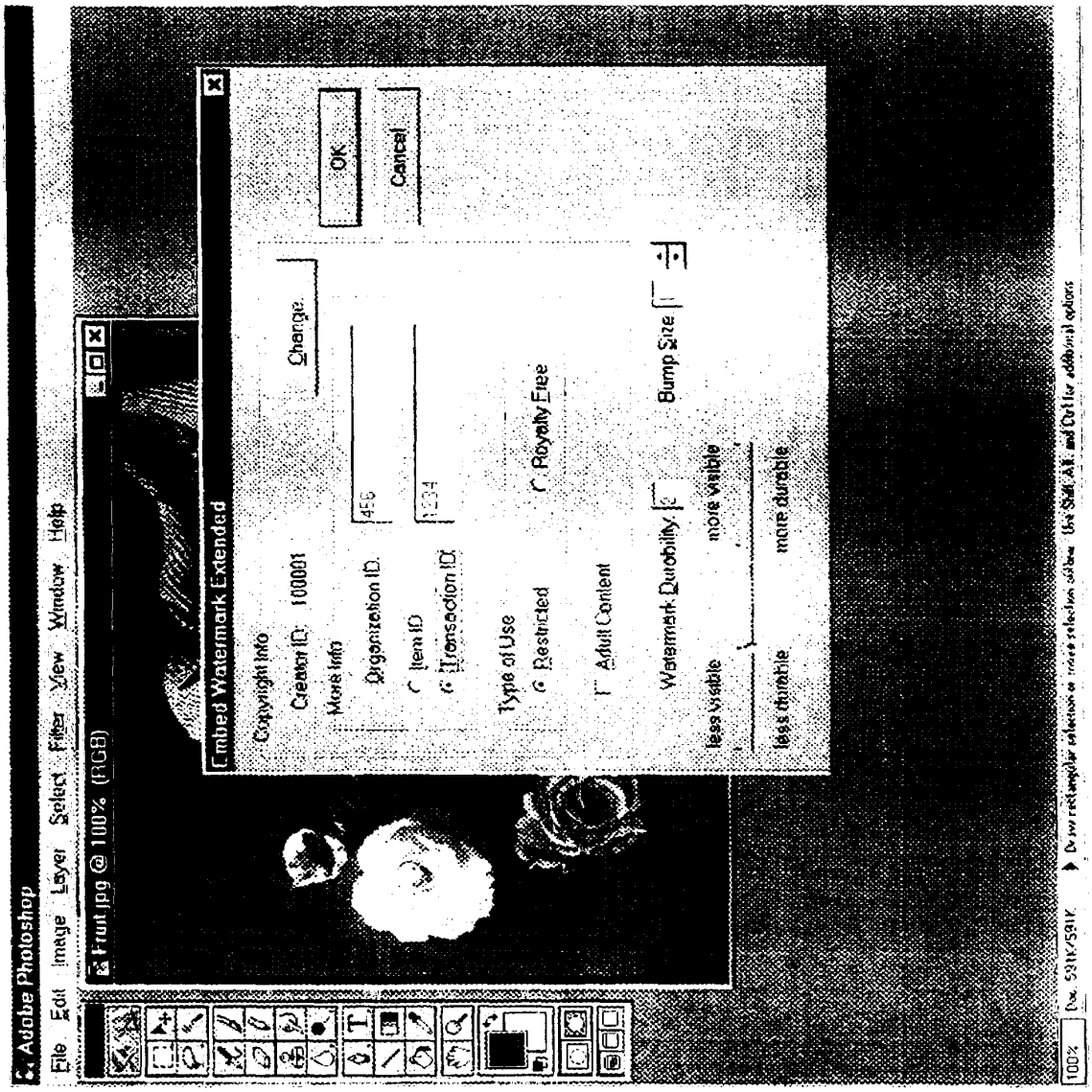

Adobe Photoshop
File Edit Image Layer Select Filter View Window Help
Fruit.jpg @ 100% (RGB)
Embed Watermark Extended
Copyright Info
Creator ID: 100001
Change...
More Info
Organization ID:
Item ID
Transaction ID:
Type of Use
Restricted
Royalty Free
Adult Content
Watermark Durability:
Bump Size
less visible
more visible
less durable
more durable
OK
Cancel

FIG. 55

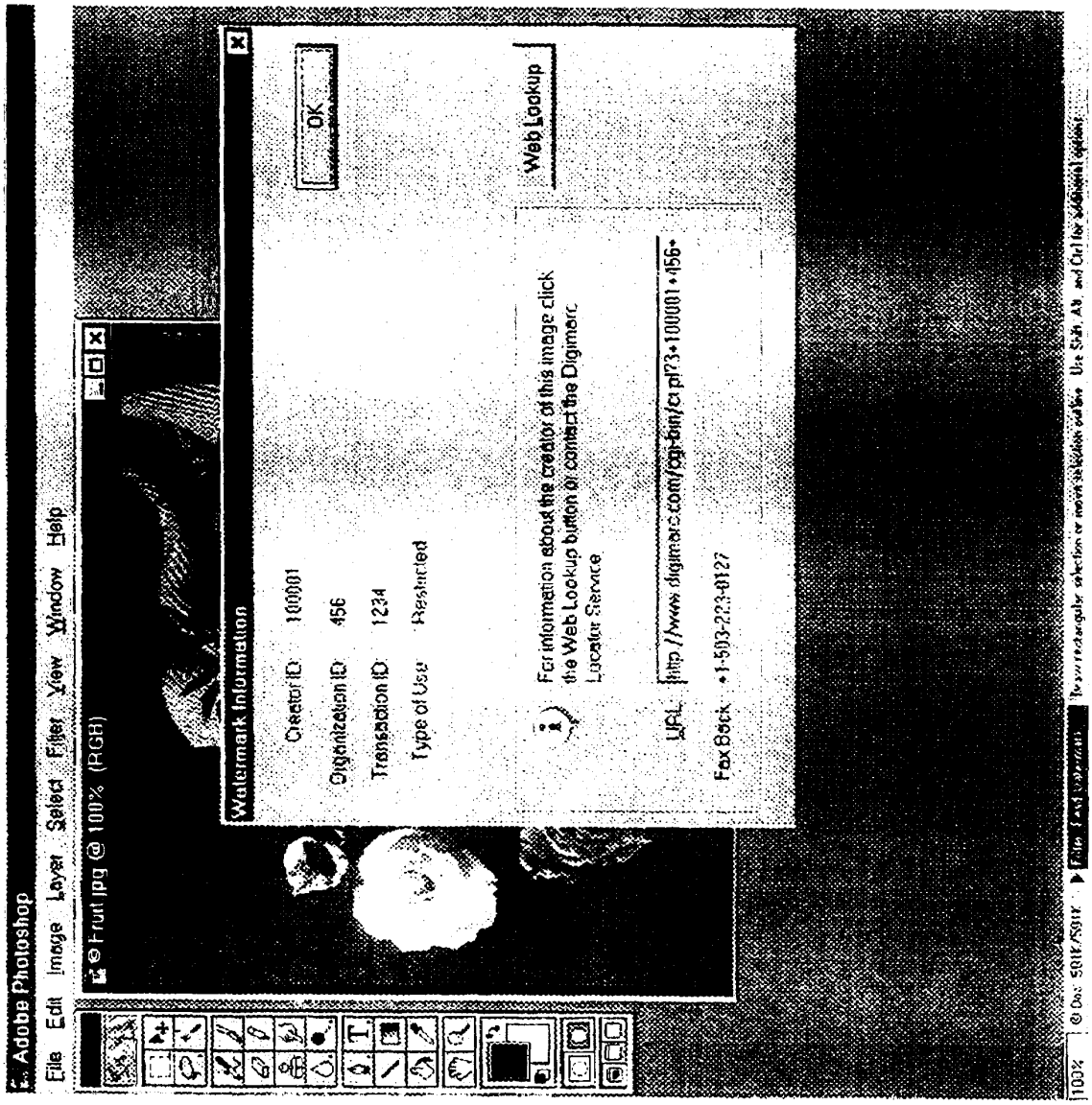

Adobe Photoshop
File Edit Image Layer Select Filter View Window Help
Fruit.jpg @ 100% (RGB)
Watermark Information
Creator ID: 100001
Digitization ID: 456
Transaction ID: 1234
Type of Use: Restricted
OK
For information about the creator of this image click the Web Lookup button or contact the Digimarc Locator Service
Web Lookup
URL: http://www.digimarc.com/cgi-bin/ct.pl?3+100001+456+
Fax Back: +1-503-223-8127

FIG. 56

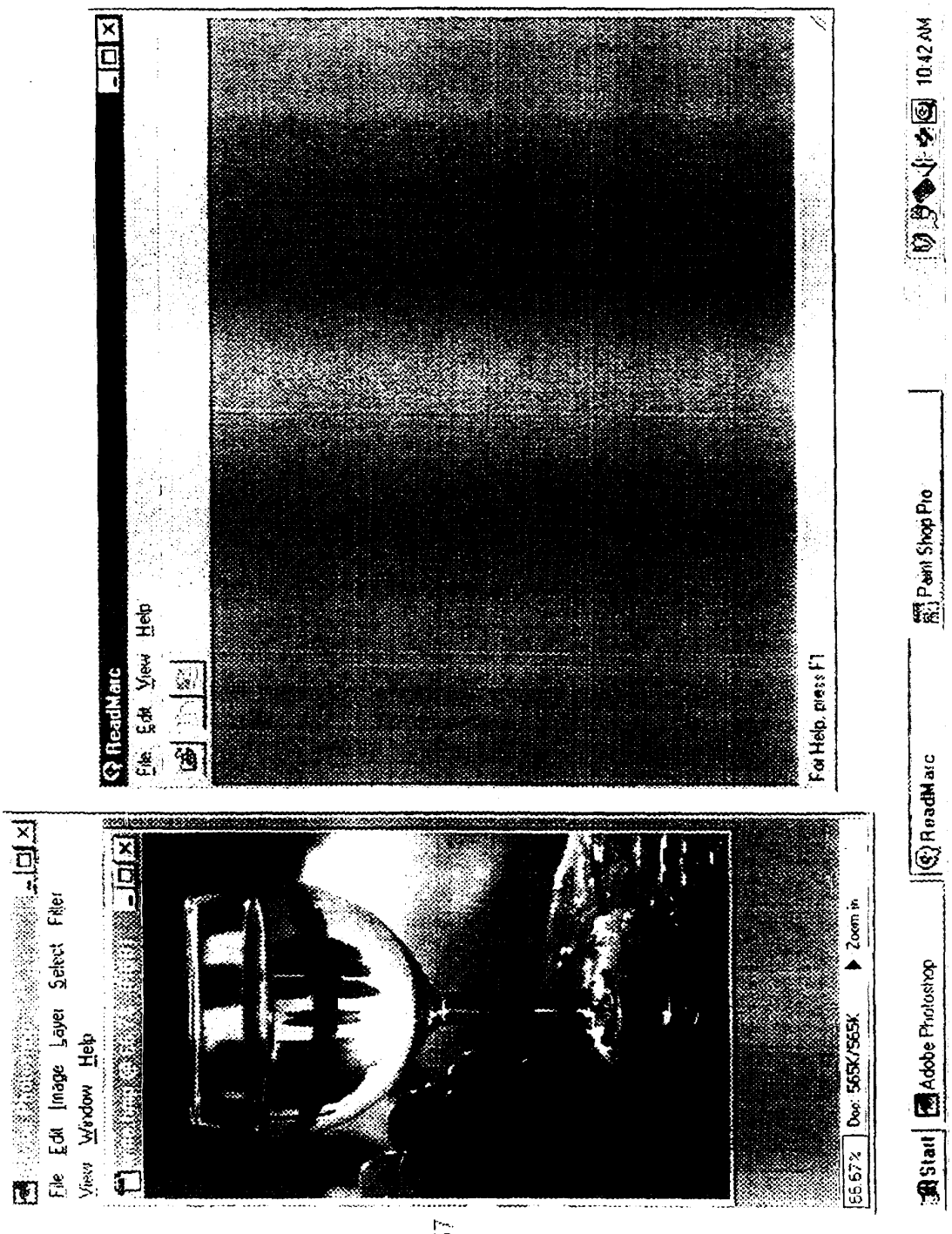

ReadMarc
File Edit View Help
For Help, press F1
File Edit Image Layer Select Filter
View Window Help
66.67%
Doc: 565K/565K
Zoom In
Start
Adobe Photoshop
ReadMarc
Paint Shop Pro
10:42 AM

FIG. 57

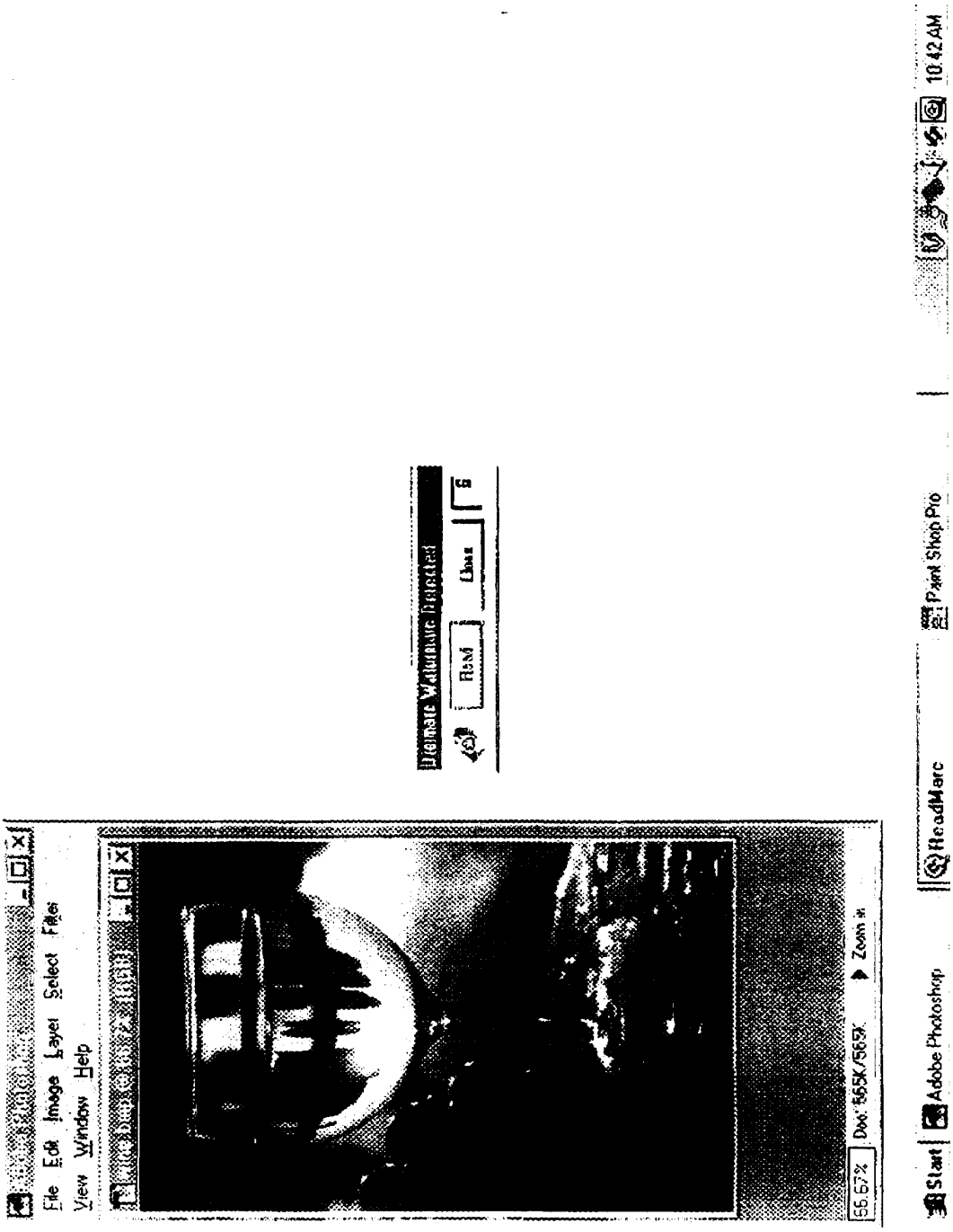

File Edit Image Layer Select Filter
View Window Help
Ordinate Waterwave Injected
Start
Adobe Photoshop
ReadMarc
Paint Shop Pro
10:42 AM

FIG. 58

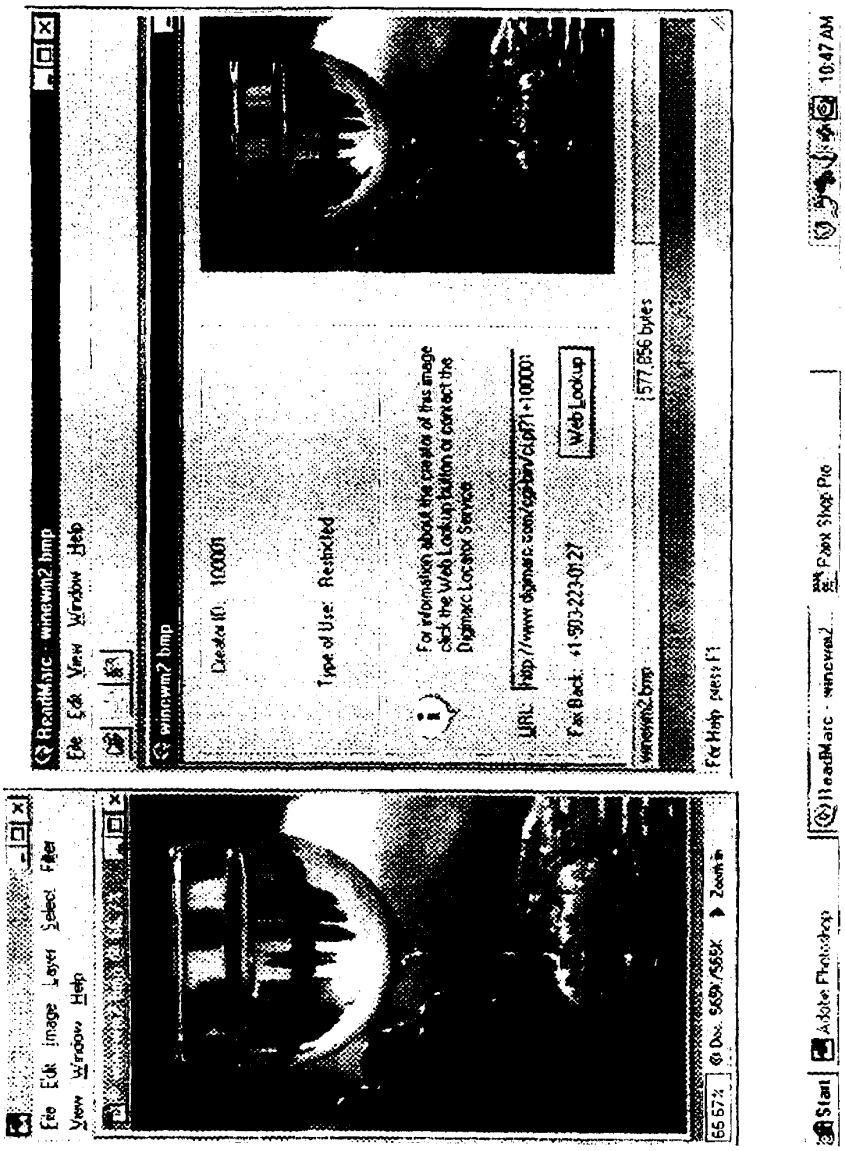

ReadMarc - winsewn2.bmp
File Edit View Window Help
winsewn2.bmp
Creator ID: 10000
Type of User: Restricted
For information about the creator of this image click the Web Lookup button or contact the Digimarc Locator Service
URL: http://www.digimarc.com/cgi-bin/cgi.pl?1+10000
For Back: +1-503-223-0127
Web Lookup
577,856 bytes
For Help press F1
File Edit Image Layer Select Filter
View Window Help
Start
Adobe Photoshop
ReadMarc - winsewn2...
Paint Shop Pro
10:47 AM

FIG. 59

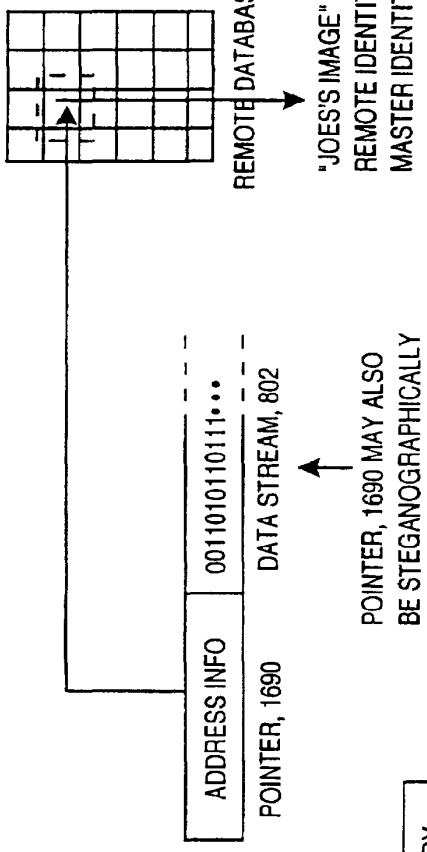

ADDRESS INFO
001101011011...
POINTER, 1690
DATA STREAM, 802
REMOTE DATABASE, 1692
"JOES'S IMAGE"
REMOTE IDENTITY,
MASTER IDENTITY, 1694
POINTER, 1690 MAY ALSO
BE STEGANOGRAPHICALLY
EMBEDDED IN DATA
STREAM IF DATA STREAM
IS SO CAPABLE
RUDIMENTARY
MASTER IDENTITY
OBJECT AND
SYSTEM

FIG. 60

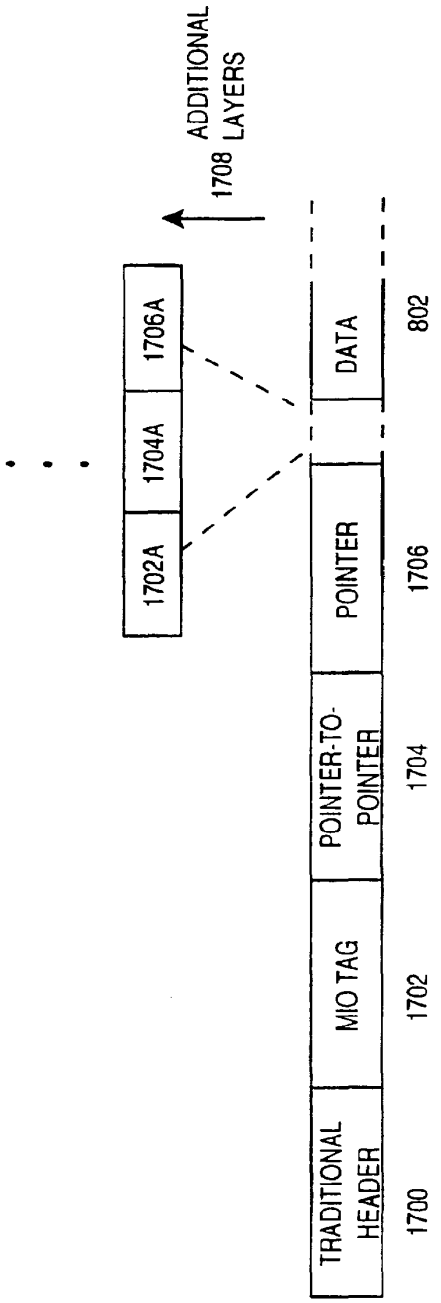

ADDITIONAL
1708 LAYERS
1702A
1704A
1706A
TRADITIONAL
HEADER
MIO TAG
POINTER-TO-
POINTER
POINTER
DATA
1700
1702
1704
1706
802

FIG. 61

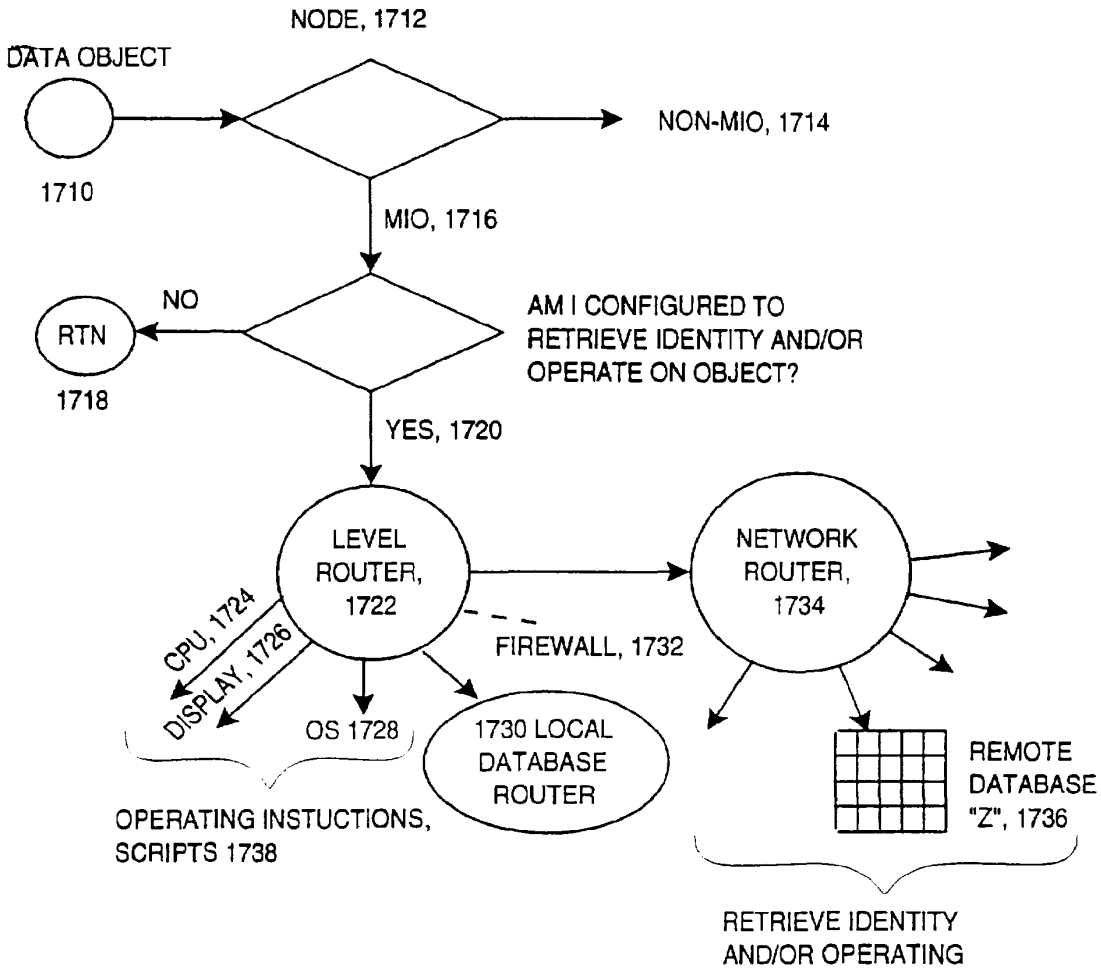

NODE, 1712
DATA OBJECT
1710
NON-MIO, 1714
MIO, 1716
NO
RTN
1718
AM I CONFIGURED TO RETRIEVE IDENTITY AND/OR OPERATE ON OBJECT?
YES, 1720
LEVEL ROUTER, 1722
NETWORK ROUTER, 1734
CPU, 1724
DISPLAY, 1726
FIREWALL, 1732
OS 1728
1730 LOCAL DATABASE ROUTER
REMOTE DATABASE "Z", 1736
OPERATING INSTUCTIONS, SCRIPTS 1738
RETRIEVE IDENTITY AND/OR OPERATING

FIG. 62

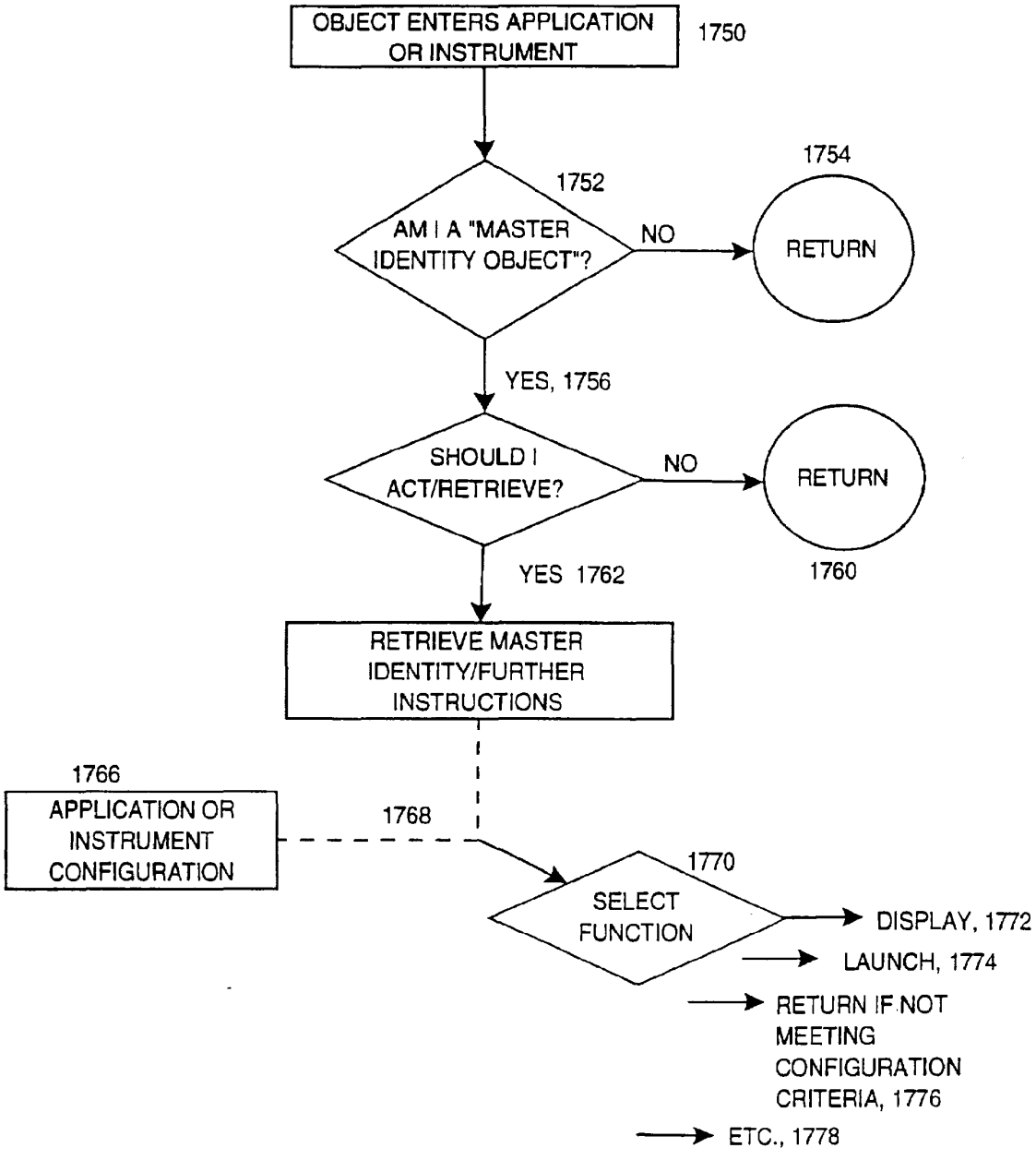

OBJECT ENTERS APPLICATION OR INSTRUMENT
1750
1752
AM I A "MASTER IDENTITY OBJECT"?
NO
1754
RETURN
YES, 1756
SHOULD I ACT/RETRIEVE?
NO
RETURN
1760
YES 1762
RETRIEVE MASTER IDENTITY/FURTHER INSTRUCTIONS
1766
APPLICATION OR INSTRUMENT CONFIGURATION
1768
1770
SELECT FUNCTION
DISPLAY, 1772
LAUNCH, 1774
RETURN IF NOT MEETING CONFIGURATION CRITERIA, 1776
ETC., 1778

FIG. 63

ATTACHED INFO
EMBEDDED SCRIPT
DATA STREAM
1800
1802
1804
ATTACHED INFO
POINTER TO SCRIPT
DATA STREAM
1800
1806
1804
REMOTE DATABASE, 1808

FIG. 64

1820
DATA OBJECT
1822
"REPORTING MODE"
MIO? 1824
YES
NO
MAY I SEND A MESSAGE TO MASTER IDENTITY? 1832
1834
YES
SEND MESSAGE TO REMOTE DATABASE, 1838
REPORT NON-HIT? 1826
YES
NO
MIO SYSTEMS STATS DATABASE, 1830
1828
RTN

FIG. 65

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/08351

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G06K 9/36
US CL :382/232
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 382/232, 284; 395/135; 358/454,448; 380/4,23,25,54; 283/6,93,94; 358/142,124,450; 348/475; 235/494

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 581 317 A2 (POWELL ET AL.) 02 FEBRUARY 1994, PAGES 1-6, FIGURES 1-5	1-5

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 17 SEPTEMBER 1997	Date of mailing of the international search report 31 OCT 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JOSE L. COUSO Toni Hill Telephone No. (703) 305-4700

Form PCT/ISA/210 (second sheet)(July 1992)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/08351

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-5

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet(1))(July 1992)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/08351

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I, claim(s) 1-5, drawn to a multi-computer system.
Group II, claim(s) 6-13, drawn to a sub-system for embedding information.
Group III, claim(s) 14, drawn to an image processing method.

The inventions listed as Groups I-III do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: The claims of these three groups are directed to different inventions which are not so linked as to form a single general inventive concept since they recite different technical features. The inventions are not linked in operation and perform completely different operations, such as Group I, a multi-computer system, Group II, a system for embedding information, and Group III, an image processor.

Since applicant has not exercised the option, the International Preliminary Authority will establish the international preliminary examination report on those parts of the international application indicated below which are claimed first, namely Claims 1-5.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/30	A1	(11) International Publication Number: WO 96/26494
		(43) International Publication Date: 29 August 1996 (29.08.96)

(21) International Application Number: PCT/US96/02357

(22) International Filing Date: 22 February 1996 (22.02.96)

(30) Priority Data:
08/392,624 23 February 1995 (23.02.95) US

(71) Applicant: THE REGENTS OF THE UNIVERSITY OF CALIFORNIA [US/US]; Business and Patent Law, Mail Stop D412, Los Alamos, NM 87545 (US).

(71)(72) Applicants and Inventors: SANDFORD, Maxwell, T., II [US/US]; 160 Monte Rey Street, Los Alamos, NM 87544 (US). HANDEL, Theodore, G. [US/US]; 316 Bryce Avenue, Los Alamos, NM 87544 (US).

(74) Agents: WYRICK, Milton, D. et al.; Los Alamos National Laboratory, Mail Stop D412, Los Alamos, NM 87545 (US).

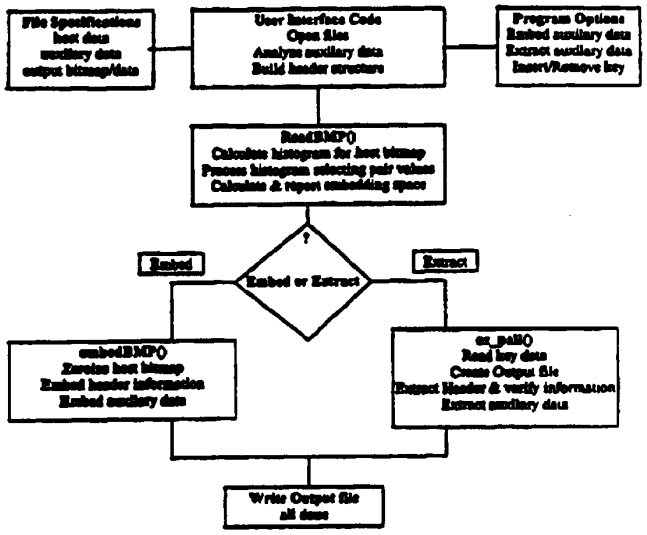
(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DATA EMBEDDING

(57) Abstract

A method of embedding auxiliary information into a set of host data, such as a photograph, television signal, facsimile transmission, or identification card. All such host data contain intrinsic noise, allowing pixels in the host data which are nearly identical and which have values differing by less than the noise value to be manipulated and replaced with auxiliary data. As the embedding method does not change the elemental values of the host data, the auxiliary data do not noticeably affect the appearance or interpretation of the host data. By a substantially reverse process, the embedded auxiliary data can be retrieved easily by an authorized user.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

DATA EMBEDDING

FIELD OF THE INVENTION

The present invention generally relates to digital manipulation of numerical data and, more specifically, to the embedding of external data into existing data fields. This invention was made with Government support under Contract No. W-7405-ENG-36 awarded by the U.S. Department of Energy. The Government has certain rights in the invention.

The use of data in digital form is revolutionizing communication throughout the world. Much of this digital communication is over wire, microwaves, and fiber optic media. Currently, data can be transmitted flawlessly over land, water, and between satellites. Satellites in orbit allow communication virtually between any two points on earth, or in space.

In many situations, it may be of benefit to send particular secondary data along with the primary data. Secondary data could involve the closed captioning of television programs, identification information associated with photographs, or the sending of covert information with facsimile transmissions. Such a technique is suited also for use as a digital signature verifying the origin and authenticity of the primary data.

Data in digital form are transmitted routinely using wide band communications channels. Communicating in digital fashion is facilitated greatly by error-correcting software and hardware protocols that provide absolute data fidelity. These communication systems ensure that the digital bit stream transmitted by one station is received by the other station unchanged.

However, most digital data sources contain redundant information and intrinsic noise. An example is a digital image generated by scanning a photograph, an original work of electronic art, or a digitized video signal. In the scanning or digital production process of such images, noise is introduced in the digital rendition. Additionally, image sources, such as photographic images and identification cards, contain noise resulting from the grain structure of the film, optical aberrations, and subject motion. Works of art contain noise which is introduced by brush strokes, paint texture, and artistic license.

Redundancy is intrinsic to digital image data, because any particular numerical value of the digital intensity exists in many different parts of the image. For example, a given grey-level may exist in the image of trees, sky, people or other objects. In any digital image, the same or similar numerical picture element, or pixel value, may represent a variety of image content. This means that pixels having similar numerical values and frequency of occurrence in different parts of an image can be interchanged freely, without noticeably altering the appearance of the image or the statistical frequency of occurrence of the pixel values.

Redundancy also occurs in most types of digital information, whenever the same values are present more than once in the stream of numerical values representing the information. For a two-color, black and white FAX image, noise consists of the presence or absence of a black or white pixel value. Documents scanned into black and white

BITMAP® format contain runs of successive black (1) and white (0) values. Noise in these images introduces a variation in the length of a pixel run. Runs of the same value are present in many parts of the black and white image, in different rows. This allows the present invention also to be applied to facsimile transmissions.

The existence of noise and redundant pixel information in digital data permits a process for implanting additional information in the noise component of digital data. Because of the fidelity of current digital communication systems, the implanted information is preserved in transmission to the receiver, where it can be extracted. The embedding of information in this manner does not increase the bandwidth required for the transmission because the data implanted reside in the noise component of the host data. One may convey thereby meaningful, new information in the redundant noise component of the original data without it ever being detected by unauthorized persons.

It is therefore an object of the present invention to provide apparatus and method for embedding data into a digital information stream so that the digital information is not changed significantly.

It is another object of the present invention to provide apparatus and method for thwarting unauthorized access to information embedded in normal digital data.

Additional objects, advantages and novel features of the invention will be set forth in part in the description which follows, and in part will become apparent to those skilled in the art upon examination of the following or may

be learned by practice of the invention. The objects and advantages of the invention may be realized and attained by means of the instrumentalities and combinations particularly pointed out in the appended claims.

BACKGROUND OF THE INVENTION

Additional objects, advantages and novel features of the invention will be set forth in part in the description which follows, and in part will become apparent to those skilled in the art upon examination of the following or may be learned by practice of the invention. The objects and advantages of the invention may be realized and attained by means of the instrumentalities and combinations particularly pointed out in the appended claims.

SUMMARY OF THE INVENTION

In accordance with the purposes of the present invention there is provided a method of embedding auxiliary data into host data comprising the steps of creating a digital representation of the host data consisting of elements having numerical values and containing a noise component; creating a digital representation of the auxiliary data in the form of a sequence of bits; evaluating the noise component of the digital representation of the host data; comparing elements of the host data with the noise component to determine pairs of the host elements having numerical values which differ by less than said value of said noise component; and replacing individual values of the elements with substantially equivalent values from said pairs of elements in order to embed individual bit values of the auxiliary data corresponding to the sequence of bits of

the auxiliary data; and outputting the host data with the auxiliary data embedded into the host data as a file.

In accordance with the purposes of the present invention there is further provided a method of extracting embedded auxiliary data from host data containing a noise component comprising the steps of extracting from the host data a bit sequence indicative of the embedded auxiliary data, and which allows for verification of the host data; interpreting the host data-element pairs which differ by less than the value of the noise component and which correspond to bit values of the auxiliary data;identifying the auxiliary data bit sequence corresponding to the pair values; and extracting the auxiliary data as a file.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and form a part of the specification, illustrate the embodiments of the present invention and, together with the description, serve to explain the principles of the invention. In the drawings:

FIGURE 1 is a block diagram illustrating the processes used in the embedding and extraction of data from a host.

FIGURE 2 is a partial listing of computer code used for determining host data pairs having similar values and for converting RGB components to HSI components.

FIGURE 3 is a partial listing of computer code used for eliminating duplicate host data pairs.

FIGURE 4 is a partial listing of computer code which, for Truecolor images, introduces a constraint on the frequency of occurrence of host data pairs that minimizes the effect of embedding on the host data histogram.

FIGURE 5 is a partial listing of computer code that performs the actual embedding of auxiliary data into the host data, including the considerable information which is necessary to manipulate the data in the header information, auxiliary bit-stream, and the host data files.

FIGURE 6 is a partial listing of computer code that analyzes the lengths of runs in a row of pixels in two-color facsimile host data.

FIGURE 7 is a partial listing of computer code whose purpose is to ensure that the first pixel in a PACKET-START data row starts in an even column number. The location of the first pixel in the row flags the start of the data packets.

FIGURE 8 is a partial listing of computer code for embedding data into two-color host images, such as facsimile transmissions.

DETAILED DESCRIPTION

The present invention allows data to be embedded into a digital transmission or image without naturally discernible alteration of the content and meaning of the transmission or image. This is made possible because of the technique of the present invention, in which similar pixel values in a set of digital host data are re-ordered according to the desired embedded or implanted information. The host data image examples are represented in the MICROSOFT® BITMAP® (.BMP) format, so that the resulting image contains the embedded auxiliary information without that information being readily discernible.