(a) a wireless device interconnected to the computer network;

(b) a list server interconnected to the computer network, the list server comprising a storage means;

(c) a client device interconnected to the computer network; wherein

the wireless device comprises:

means for inputting a linkage code comprising a routing identification code and an item identification code;

means for transmitting the linkage code in a data stream to the list server for storage therein, wherein said data stream includes a subscriber identification number associated with the wireless device; and

the client device comprises:

means for logging into the list server and providing the subscriber identification number of the linkage code stored on the list server; and

means for retrieving the linkage code from the list server.

62. The system of claim 61, wherein the client device further comprises means for a user to provide the client device with the subscriber identification number.

63. The system of claim 61, wherein the client device is one of a group of devices comprising a personal computer, a web-based television, and a video console.

64. The system of claim 61, further comprising means for utilizing the linkage code to enable the client device to retrieve a primary content file associated with the item identification code from a content server associated with the routing identification code.

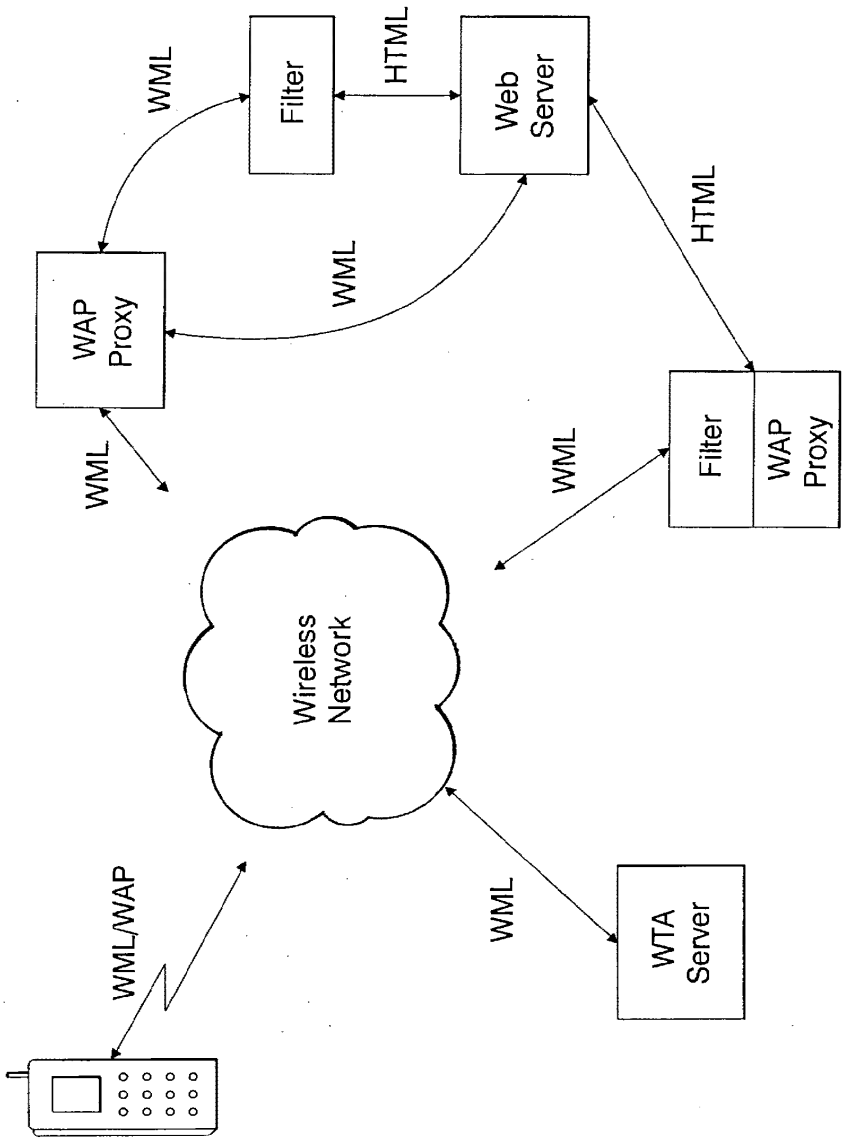

WML
Filter
HTML
Web Server
WAP Proxy
WML
HTML
WML
Filter
WAP Proxy
WML
Wireless Network
WML/WAP
WML
WTA Server

FIG. 1

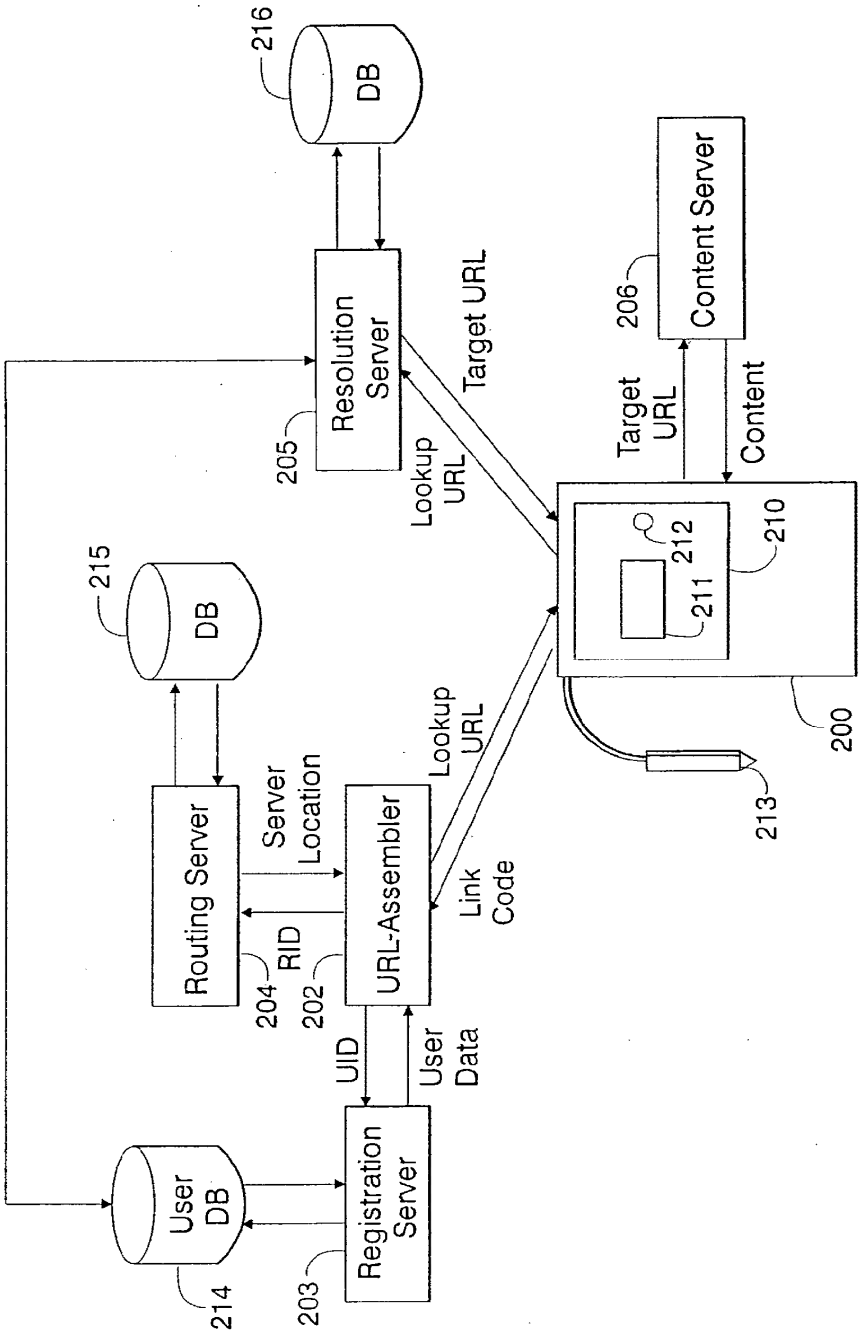

216
DB
Resolution Server
205
Target URL
Lookup URL
206
Content Server
Target URL
Content
215
DB
212
211
210
200
213
Routing Server
Server Location
RID
204
202
URL-Assembler
Lookup URL
Link Code
UID
User Data
User DB
214
Registration Server
203

FIG. 2

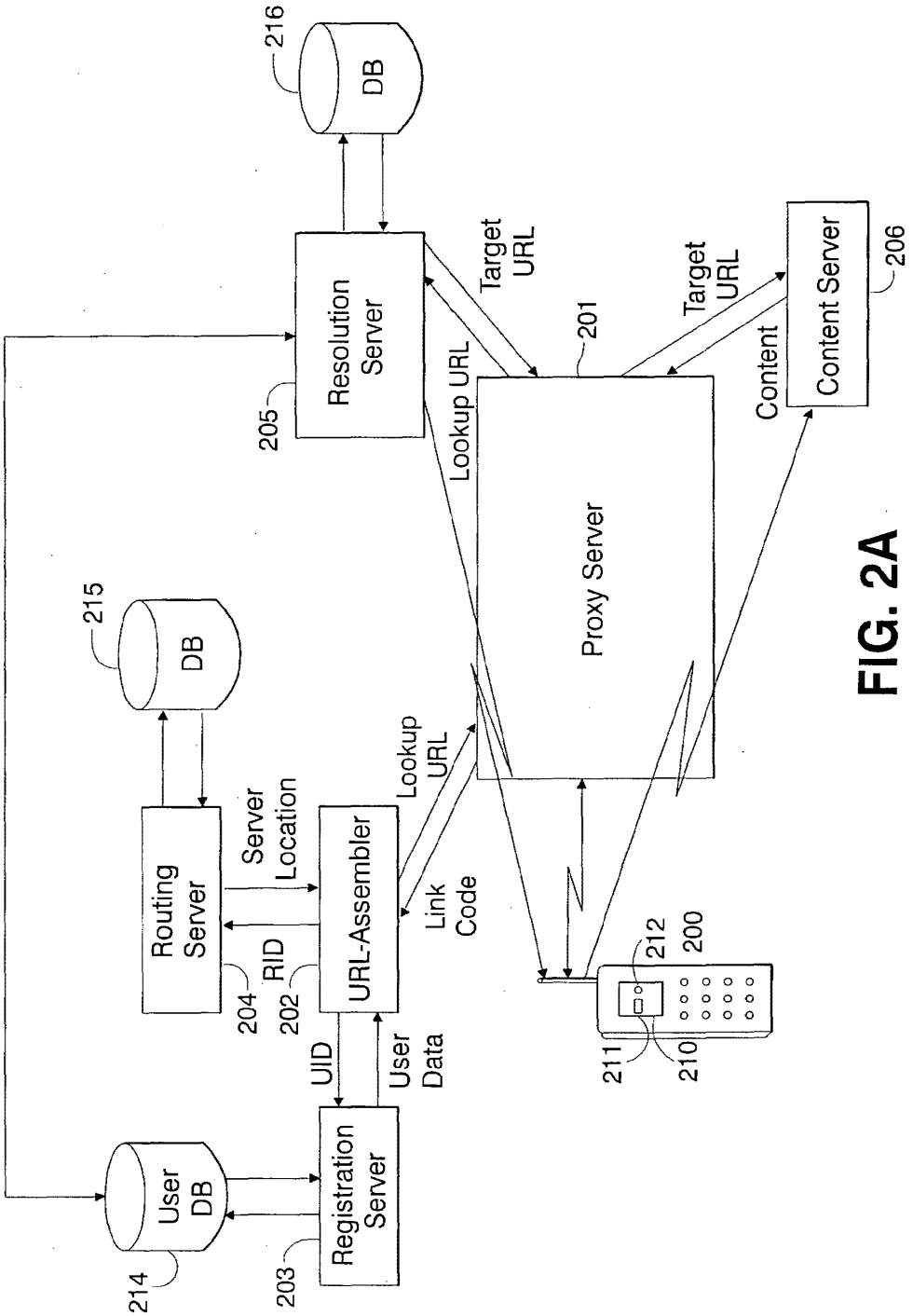

216
DB
Resolution Server
205
Target URL
Lookup URL
201
Target URL
Content
Content Server
206
Proxy Server
215
DB
Routing Server
204
Server Location
RID
202
URL-Assembler
Lookup URL
Link Code
212
200
211
210
UID
User Data
User DB
214
Registration Server
203

FIG. 2A

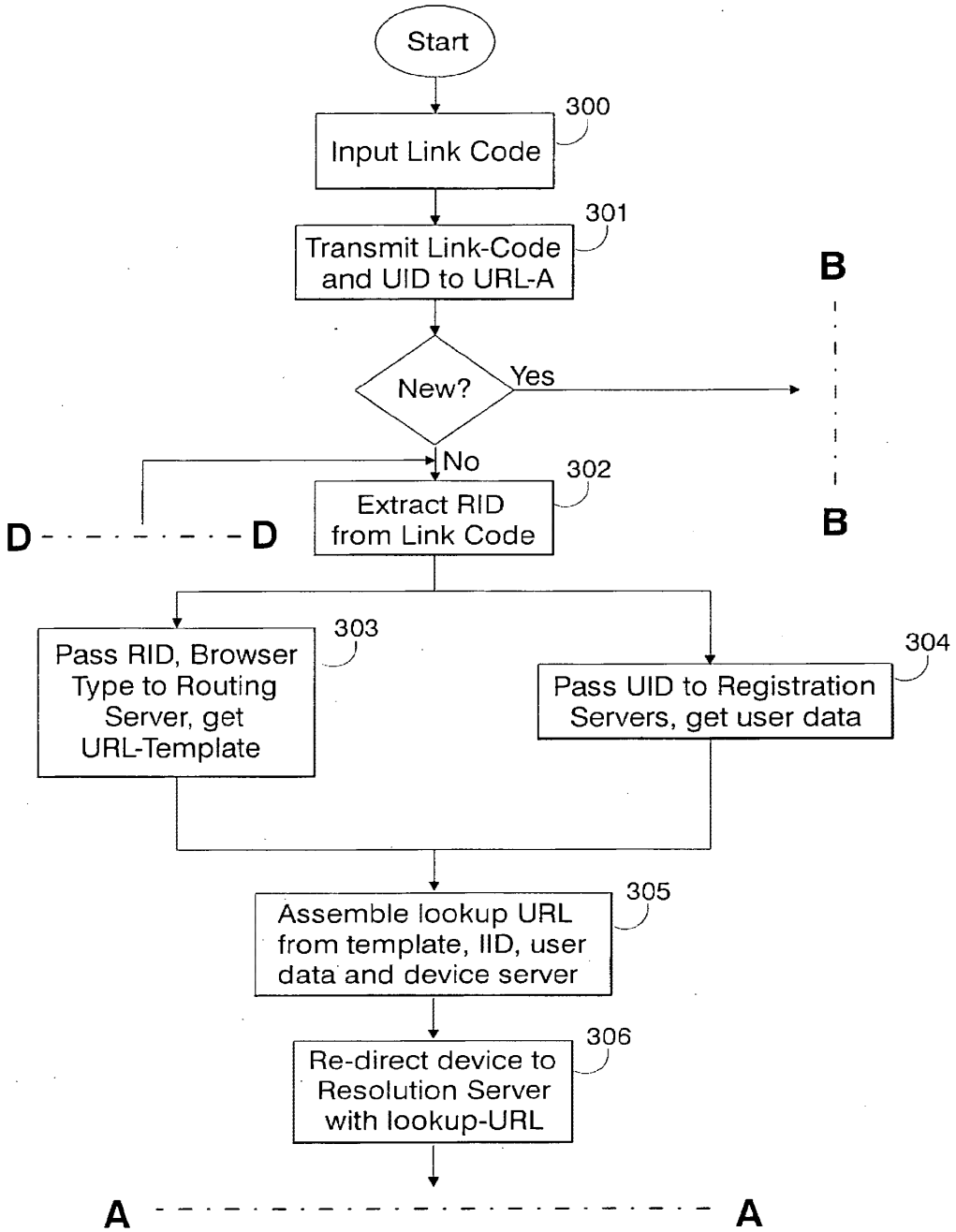

Start
300
Input Link Code
301
Transmit Link-Code and UID to URL-A
B
New?
Yes
No
302
Extract RID from Link Code
D
D
B
303
Pass RID, Browser Type to Routing Server, get URL-Template
304
Pass UID to Registration Servers, get user data
305
Assemble lookup URL from template, IID, user data and device server
306
Re-direct device to Resolution Server with lookup-URL
A
A

FIG. 3A

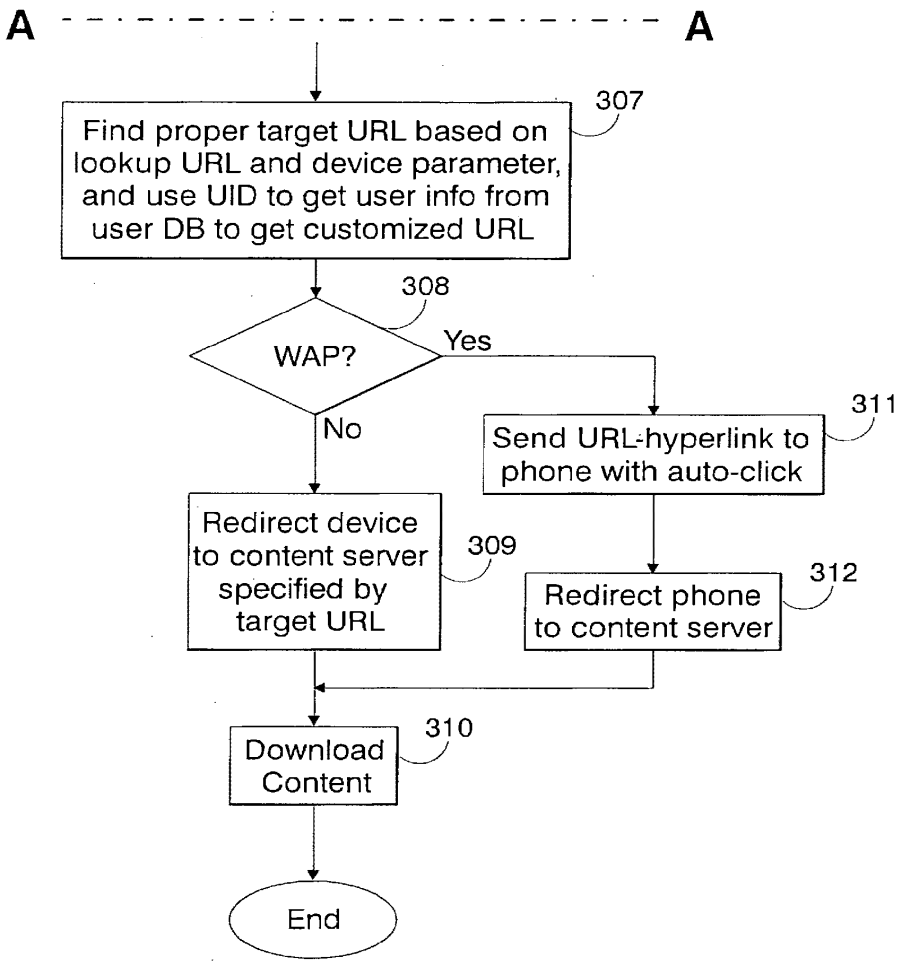

A
A
Find proper target URL based on lookup URL and device parameter, and use UID to get user info from user DB to get customized URL
307
WAP?
308
Yes
No
Send URL-hyperlink to phone with auto-click
311
Redirect device to content server specified by target URL
309
Redirect phone to content server
312
Download Content
310
End

FIG. 3B

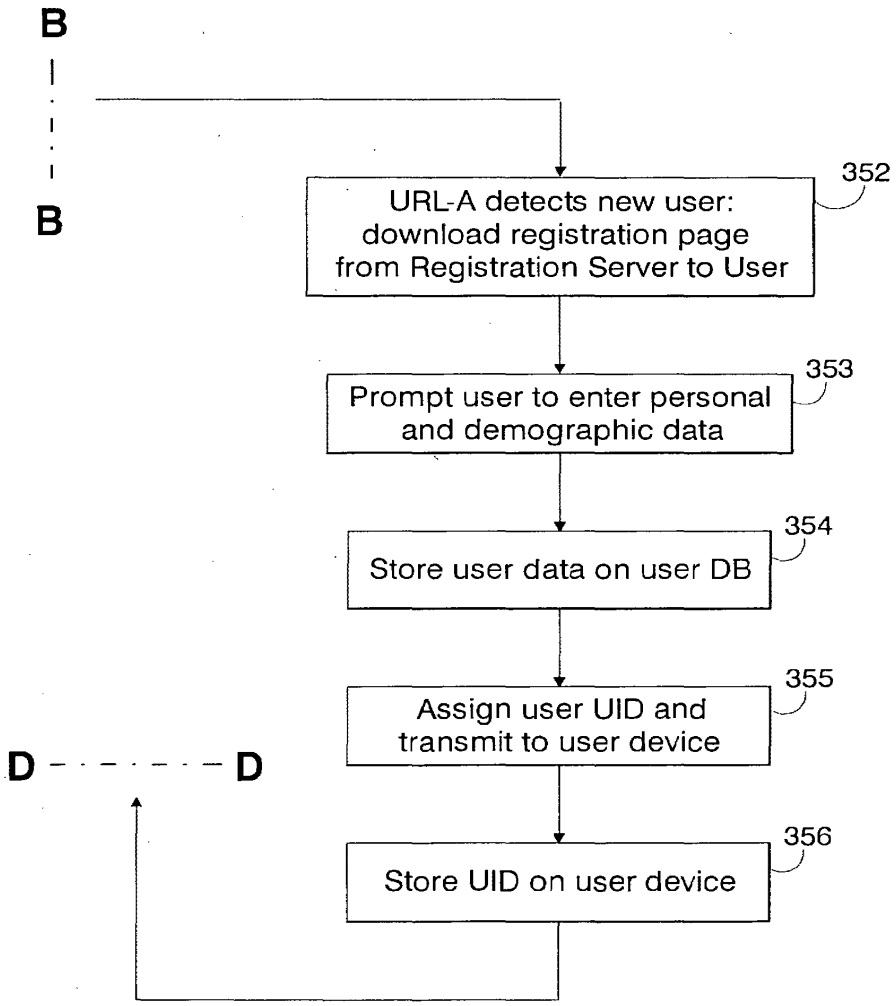

B
B
URL-A detects new user: download registration page from Registration Server to User
352
Prompt user to enter personal and demographic data
353
Store user data on user DB
354
Assign user UID and transmit to user device
355
D
D
Store UID on user device
356

FIG. 3C

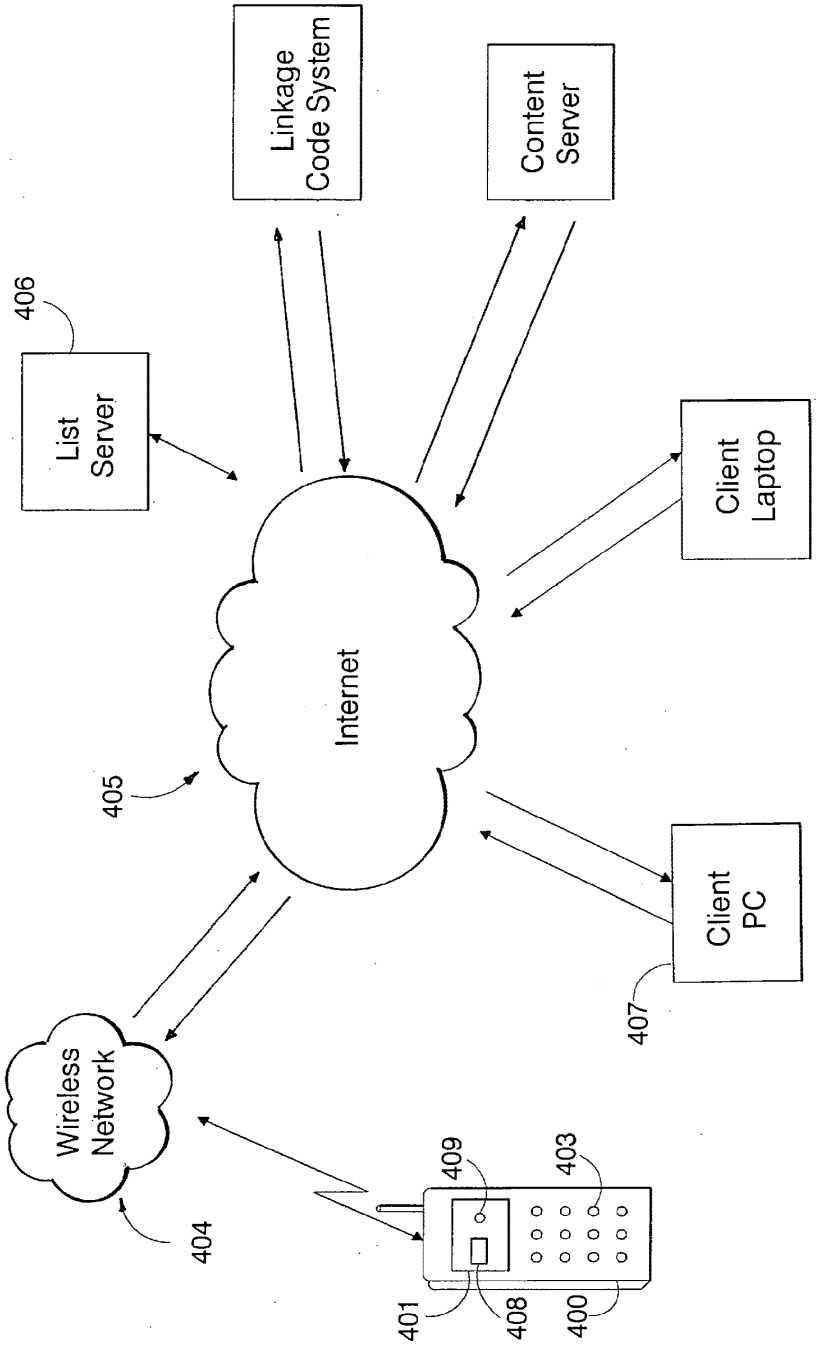

Linkage Code System
Content Server
406
List Server
Client Laptop
Internet
405
Client PC
407
Wireless Network
404
409
403
401
408
400

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/10336

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :GO6F 15/16, 15/173
US CL :709/219, 229

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. : 709/219, 229

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)

WEST, STN, IEEE

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 5,804,803 A (CRAGUN et al.) 08 SEPTEMBER 1998, Fig. 1, 1B, an abstract, col. 2, lines 45-55, col. 5, lines 50-65, cols. 6-12	1, 23, 45, 51, 57, 61 --- 2-22, 24-44, 46-50, 52-56, 58-60, 62-64
Y	US 5,905,248 A (RUSSELL et al.) 18 MAY 1999, an abstract, Figs. 1 and 3, cols. 25-28.	1-64
Y	US 5,933,829 A (DURST et al.) 03 AUGUST 1999, an abstract, Figs. 1-3, cols. 10-14.	1-64
Y	US 5,986,651 A (REBER et al.) 16 NOVEMBER 1999, an abstract, Figs. 1-6, cols. 20-24.	1-64

[X] 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 31 MAY 2001	Date of mailing of the international search report **28 JUN 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 KRISNA LIM Telephone No. (703)-305-9672

Form PCT/ISA/210 (second sheet) (July 1998)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/10336

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US 6,064,979 A (PERKOWSKI) 16 MAY 2000, an abstract, Figs. 1, 1A, cols. 22-28.	1-64

Form PCT/ISA/210 (continuation of second sheet) (July 1998)★

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 December 2001 (20.12.2001)

PCT

(10) International Publication Number
WO 01/97128 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/KR01/00997

(22) International Filing Date: 11 June 2001 (11.06.2001)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
2000/31945 10 June 2000 (10.06.2000) KR

(71) Applicant *(for all designated States except US)*: **MARKANY INC.** [KR/KR]; Ssanglim Bldg. 10Fl., 151-11, Ssanglim-dong, Chung-gu, Seoul 100-400 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CHOI, Jong-Uk** [KR/KR]; 2-1301 Seongwon APT., 1, Wooi-dong, Dobong-gu, Seoul 142-090 (KR). **LEE, Won-Ha** [KR/KR]; 106-1704, Ssangryong APT., 64, Imun 3-dong, Dongdaemun-gu, Seoul 130-083 (KR).

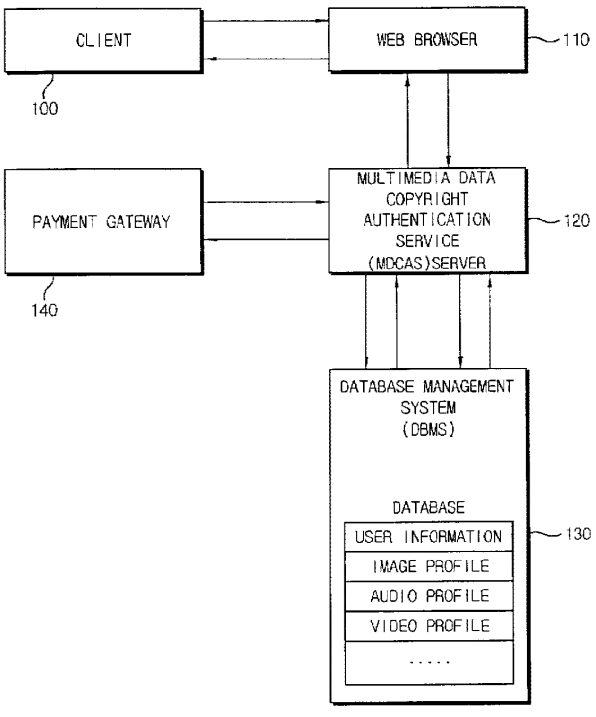
(74) Agent: **KOREANA PATENT FIRM**; Dong-Kyong Bldg. 824-19, Yoksam-dong, Kangnam-ku, Seoul 135-080 (KR).

(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, 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).

[Continued on next page]

(54) Title: SYSTEM AND METHOD OF PROVIDING AND AUTHENTICATING WORKS OF AUTHORSHIP BASED ON WATERMARK TECHNIQUE



(57) Abstract: The supply of works of authorship and their authentication are provided by a service system and method for supplying and authenticating digital data works of authorship based on a watermarking system. The works of authorship including invisible information on a copyright is provided through this system. In the event that illegal use of original works of authorship is sensed, the illegal copy and use of multimedia contents could be prevented by presenting accurate technical evidence to support the information on a copyright through authentication of an authentication organization and thereby the protection of a copyright is possible. Authentication of a copyright of the contents is performed by the steps of imbedding and extracting of a digital watermark such as a logo or signature of a copyright holder on a data.

WO 01/97128 A1

Published:
— *with international search 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.

SYSTEM AND METHOD OF PROVIDING AND AUTHENTICATING WORKS OF AUTHORSHIP BASED ON WATERMARK TECHNIQUE

Technical Field

The present invention relates to a service system and method for supplying and authenticating a copyright based on a method and device, in which a watermark is embedded into the data of a digital content (digital image, digital audio, digital video, digital document, etc.) and the embedded watermark is extracted. More particularly, this invention relates to a service system and method for supplying and authenticating a copyright, which are capable of protecting a copyright of original data by selling or providing data, in which copyright information is hidden in an image watermark form, to users on the internet, and settling copyright-involved distribution by using an authentication result from a comparison of information extracted from the hidden copyright information with the copyright information previously registered in a certificate authority, thereby preventing illegal copying and distribution of the data.

Description of Prior Art

With the recent rapid spread of internet services, the population of internet users in Korea reached 14.8 millions as of the end of 1999. Under such circumstances of sharp growing Internet, presently, information such as text, still images and simple moving pictures is mainly in distribution. However, owing to the spread of various forms of video/audio transmission media, internet transmission of all sorts of multimedia data is on an increasing trend.

Meanwhile, it is believed that papers, magazines, audio, radio, TV programs,

and electronic libraries presently being operated free on the internet will be converted to chargeable services in the future. Domestic content providers are pushing forward chargeable services of contents centering on small payment service companies and PC telecommunication companies. According to such tendency, providers of digital information or content owners will need to assert and protect their copyrights on the information (digital copyrighted materials such as images, audio, video, etc.) they own, and request a reasonable compensation for use in the case of providing their copyrighted materials to others.

However, digital copyrighted materials have so many problems in their copyrights protection in view of their features. Since desired information could be easily stored or converted, multiple copies of information are possible without constraint in a free-accessible space like the internet. Further, even after copying, there can be maintained the same data information as that of the original, moreover, its distribution is possible without a copyright owner's consent, and thus copyright protection of a copyright owner is difficult.

As such, copyright infringements are increasing day by day, many legal, systemic and technical resolutions to solve these problems have been formulated. For this purpose, there are provided certain technical solutions, such as encryption of data by which an encrypted data is available to only a specific user and a digital watermarking technique where copyright information is hidden in data, which data is then transmitted to a user without the data being deformed outwardly.

Among these technical solutions, as a watermarking is a copyright protection technique of digital data, it can be considered a copyright indication or verification technique for a digital content. This technique makes it possible to detect counterfeit

or alteration of data and assert the ownership of a copyright holder by hiding copyright information in data and extracting again the hidden copyright information.

As watermarking embedding methods, there are provided a Spatial Method in which a subtle transformation is applied to data such as pixels of a screen and the like to be used as a watermark; Discrete Cosine Transform (DCT) in which digital-type data are converted to analog signals of frequency components and then a watermark converted by the same method is embedded; Fast Fourier Transform (FFT); and a Frequency Domain Method using wavelet transform.

A watermarking technique adopted by the present invention for copyright protection is to embed a "mark" which protects the original information. Such method is divided into a visible watermarking technique perceptible to the human eye and an invisible watermarking technique imperceptible to the human eye.

As the visible watermarking technique is a type of overwriting copyright information on the original, it generally prevents a user from illegally eliminating the copyright information. However, since the copyright information is visually displayed on the original, it has a disadvantage that it is difficult to preserve the value of the original. The visible watermarking technique is technically realizable without difficulty but it damages the content, thus making it difficult to be used in the electronic business.

In contrast, since the invisible watermarking technique is invisible to the human eye, it can protect a copyright without damaging the original. Also, in case that a copyright-related problem occurs, a copyright holder can claim his copyright based on the copyright information extracted from the original. Currently most watermarking techniques employ this invisible method. Accordingly, in case where the invisible

watermarking technique is used, even if images or audio/video files are distributed across the internet, users could not perceive at all whether a watermark is embedded in the copyrighted material distributed. Even a copyright holder who embedded a watermark could not find the difference between a file before the watermark is embedded and that after the watermark is embedded.

Conventional methods for embedding/extracting a watermark are directed to "a watermarking method based on detection" that embeds a user's ID (number, name) or simple data into a copyrighted material and detects them. In such an image watermarking method, presently, the existence of a watermark is determined by measuring a correlation between a watermark-embedded image and a user ID after embedding a user ID composed of 48 bits or so binary codes into image data. That is, if the correlation coefficient shows 0, the data is determined not to include the user ID, however, if the correlation coefficient shows values other than 0, the data is determined to include the user ID. Digimarc, BlueSpike, MediaSec and AlphaTech, etc., that are now providing a watermarking technique of the image field, generally use the above method.

However, under the present circumstances that embedding or detecting work of a specific ID as a watermark is performed directly by users, a big problem is how to establish a copyright on the relevant copyrighted material or settle such dispute in the event that copyright-related disputes arise.

Also, even in a case where copyrighted material is distributed through a legal course, there is a problem such that a copyright owner could not know the extent of the use and detection of such watermark is completed.

Furthermore, even if a watermark on a copyrighted material is embedded, since

such embedment is merely performed by either a user or a copyright holder but does not contain information on the copyrighted material according to its characteristics, it is impossible to find out a distribution channel of such copyrighted material.

Also, since the aforementioned methods use a method for embedding information that has no direct relationship with a copyright as binary code, there has a limitation that it is not easy to obtain information about a copyright from copyrighted material containing an embedded watermark.

Summary of the Invention

It is therefore an object of the present invention to overcome the above-described problems in prior art. In order to protect a copyright of digital multimedia data distributed on the internet, there is provided a service system and method for supplying and authenticating copyrighted materials by providing a service capable of verifying user information using a watermark embedding and extracting method based on extraction.

It is another object of the present invention to provide a system and method for protecting a copyright of a content provider (i.e., a copyright holder, and a seller to whom a duplication right of copyrighted material is assigned from the copyright holder) by embedding a watermark including user information into various digital content data and then distributing the content containing a copyright on the internet.

It is another object of the present invention to provide a means capable of verifying and authenticating an original by applying this technique to electronic documents exchangeable on the internet (various administrative civil affair documents, contracts, principle documents of companies, electronic publications, receipts,

purchasing documents, etc.) in order that parties can safely exchange electronic documents on the internet.

It is another object of the present invention to establish the just internet business culture by preventing the loss of information and the distribution of illegally copied data on the internet, which is possible by embedding main information into digital data in a watermark form and then transmitting it.

It is another object of the present invention to discover a distribution channel of the corresponding copyrighted material by transmitting copyright-related information which is embedded as a watermark after sorting the information on a copyright holder and users.

In order to achieve the above-mentioned objects, the service system for supplying copyrighted material according to the present invention includes a database for storing information on a copyrighted materials, and a copyrighted material supplying means for supplying the copyrighted material, at a user's request through the internet, into which copyright information is embedded as a watermark, said copyrighted material being received from said database.

Further, the service system for authenticating a copyrighted material according to the present invention includes a database for storing information on the copyrighted material, and a copyrighted material authenticating means for performing authentication on the copyrighted material supplied from a user, at the user's request through the internet, after comparing on extracted watermark embedded in the copyrighted material of said user with the information on said copyrighted material stored in said database.

The service method for supplying a copyrighted material according to the present invention includes a step of registering a copyrighted material supplied by a

copyright holder through the internet and copyright information of said copyrighted material; a step of embedding said copyright information into said copyrighted material as a watermark at a user's request for the supply of said registered copyrighted material; and a step of providing the watermark-embedded copyrighted material to said user.

The service method for authenticating a copyrighted material according to the present invention includes a step of receiving a copyrighted material at a user or copyright holder's request through the internet for the authentication of the copyrighted material; a step of extracting a watermark from said received copyrighted material; and a step of transmitting the authentication result to said user or copyright holder after comparing the copyright information obtained from said extracted watermark with stored copyrighted material and copyright information.

Hereinbelow, the service system and method for supplying/authenticating copyrighted material based on the watermarking technique according to the present invention will be more concretely explained with reference to the accompanying drawings.

Brief Description of the Drawings

Fig. 1 is a block diagram schematically illustrating the constitution of a system, which supplies a copyright authentication service on digital data according to the present invention.

Fig. 2 is a block diagram, showing an instance of the service supplying system according to the present invention, which illustrates the constitution of the system, being divided into server/client sides, for supplying a watermark embedding service.

Figs. 3A and 3B are flowcharts illustrating one embodiment of the operation

method in a service supplying system according to the present invention. Fig. 3A illustrates a process for embedding a watermark and Fig. 3B illustrates a process for extracting a watermark.

Fig. 4 illustrates an instance in case where a user is allowed to select a watermarking method during a process of Fig. 3A.

Fig. 5 is a flowchart schematically illustrating a process for embedding/extracting a watermark by using various watermarking methods provided by MDCAS.

Fig. 6 is a flowchart schematically illustrating a process in which a user is allowed to directly embed a watermark and to register the watermark-embedded content in MDCAS.

Detailed Description of the Preferred Embodiments

Fig. 1 is a block diagram, which schematically illustrates the constitution of a system for supplying a copyright authentication service on digital data according to the present invention. The system of Fig. 1 includes a user system (a service requester/a user; hereinafter referred to as 'client') 100 to be accessed via the internet, a multimedia data copyright authentication server (hereinafter referred to as "server") 120 for supplying Multimedia Data Copyright Authentication Service (hereinafter referred to as MDCAS); and a web browser 110 which plays a role as an intermediary of data communication between a DataBase Management System (hereinafter referred to as DBMS) 130 for storing information about the user information and various multimedia data, and a server 120 and a client 100. Said system may include a Payment Gateway 140 for surcharging on the use of the multimedia data.

According to the system of the present invention, the supply of copyrighted material of digital data or the copyright authentication is performed in the client 100 and the server 120 as a certificate authority of the digital data copyright. The above client 100 means all systems of copyright holders who allow users to utilize their copyrighted materials by making their copyrighted materials authenticated by means of the MDCAS or by registering their copyrighted materials in the database management system, as well as users who are supplied with the copyrighted materials by using the MDCAS.

Also, for the watermarking technique used in the above system, conventional various watermarking methods are available. Also, there are available methods taught by a watermarking-related patent application filed by the applicant of the present application (Korean Patent Application No. 98-37237: Watermarking method of digital image using wavelet conversion and discrete cosine conversion; Korean Patent Application No. 37274: Watermarking method of digital image using wavelet conversion and discrete cosine conversion).

In the present invention, "an extraction-based watermarking method" will be exemplified, which is used in the above-mentioned earlier patent applications and in which an imaged watermark is embedded into the original data and then extracted. In the case of image data, the extraction-based watermarking method capable of identifying the embedded watermark after extraction with the human eye has more commercial value, rather than "a detection-based watermarking method" in which a watermark is embedded by generating a conventional random sequence, i.e., a method of determining only the embedment of a watermark by calculating a co-relationship.

In other words, since the extraction method uses symbols, such as a trademark, logo, registered seal, emblem, or an autograph already publicly authorized or known to

the public, as an authentication means, the extraction method is much easier to protect and identify a watermark than the detection method using binary codes. However, the watermarking method is not limited to such method but various methods to be determined by a content holder are available as mentioned above.

In case that it is determined to be necessary to extract and authenticate copyright information for accurate evidence, the extraction-based watermarking method to be given as an example in the present invention may be used. However, for the case of determining only whether or not a watermark exists, the detection-based watermarking method may be used, in which a random bit sequence occurred by using a key (a specific key or user key) is used as a watermark. That is, there are various watermarking methods that have been developed or are presently being developed as described above, and thus a content holder can select a method suitable for his circumstance or business. However, such developed methods are quite different from each other and their purposes to be sought also considerably differ and thus, it is now difficult to mutually endorse such methods and manage a standardized content.

In order to overcome such problems, there is recently provided a two-layer digital watermarking method. Said two-layer digital watermarking method uses a mixture of a selective watermark (called as "real watermark") and a standard watermark (called as "meta watermark"), meaning a mixed use of a meta watermark and a real watermark.

For example, it means that specific indexes provided in each of the watermarking methods are embedded into a meta watermark of 8 bits (watermarking method for company A is No. 1, and that for company B is No. 2, etc.), information of each content or information of a copyright holder, etc., can be selectively and freely

embedded into a real watermark of 16 bits. That is, this method detects what watermarking technique is used from extraction of a meta watermark, and then, selects an extraction method therefrom to detect a real watermark. The present invention may also use the above two-layer digital watermarking method in selecting a watermarking method for an authorization service.

In the system according to the present invention, there are provided two services for supplying and authenticating a copyrighted material. As one service is embedding copyright information, it can simply embed copyright information into the original data as well as store in a certificate authority such information when a user registers the embedded data in the certificate authority and whether the copyright authentication (embedment of a watermark) is completed, thereby capable of issuing authentication data containing such information at any time when the user requests it. Also, this service makes it possible to find out a distribution channel of a copyrighted material by hierarchically embedding copyright information depending on whether a user is a copyright owner of the relevant copyrighted material or a simple user utilizing the copyrighted material.

The other service is authenticating copyright information of data by detecting and extracting a watermark from watermark-embedded data.

Examining the detailed operation of such services according to the foregoing basic characteristics, a client 100 connected to a server 120, the certificate authority, exchanges data through the web browser 110 on the internet. The server 120 receives the inputted specific data through the web browser 110 from the client 100, and then, stores the data in the database within the DBMS 130 or retrieves the database to transmit the requested data to the client 100 through the web browser 110. The

database within the DBMS 130 of the certificate authority is divided into a variety of tables, for example, user information, image profiles audio profiles and video profiles, etc. The user information table stores matters for proving a person's identity, such as a user's name, ID, password, address, identification number, as well as matters about payable means in the case of using a copyright authentication service (payment method, type of cards, card number, and term of validity, etc.).

Such user information table can be classified into copyright holder information containing a content copyright and content provider information. A person who wishes to be a member of the early stage should input the above-mentioned all his user information, which is stored in the database.

A registered member, whose all user information is stored in the database, should log in by using his ID and password. That is, in case where a registered member uses the authentication service in the future, the server 120 requests the DBMS 130 to verify the user information. Then, ID and password inputted by the user are transmitted to the database in the DBMS. In this case, according to the consistency or inconsistency of the information stored in the database and the information inputted, the result is transmitted to the server 120 and outputted to the user though the web browser 110.

Also, when a service is used, a service charge is paid by a registered payment means among the stored user information. For this purpose, in case where a user utilizes a service of the present invention, the authentication system of the present invention comprises a means for transmitting an itemized use statement to the payment gateaway 140 so that the user can pay his service charge. In addition, in order to provide the system of the present invention on the web, it is desirable that a united

platform interface such as an ActiveX control be provided to a user utilizing MDCAS.

For a watermark embedding method for providing copyrighted material for which a copyright is authenticated, there are provided a case where a watermark embedding process is performed by a user and an other case where the watermark embedding is performed by a certificate authority at a user's request. First, in the case of watermarking by the certificate authority, if a user transmits the original copyrighted material to the certificate authority (via on-line or off-line), then the certificate authority embeds a watermark image including a user's logo requested into the original copyrighted material and then transmits the watermark-embedded data to the user. Regardless of the place of watermarking, the user can distribute the watermarked data, not the original copyrighted material, on the internet.

For the performance of a watermarking by the certificate authority, a user should first register himself or his logo with the certificate authority. The processes of membership registration and logo registration will be needed in the future when providing a service for extracting a watermark from a watermark-embedded copyrighted material, and which are a registration procedure for authenticating a copyright. A logo of the present specification can be used as an identifier of a user such as an individual signature or a company's logo, and thus it is desirable that the logo be easily recognizable in the form of images. Therefore, it is desirable that a watermark to be embedded into a copyrighted material include a logo image together with additional information.

Likewise, in case where a user directly embeds a watermark, the user must register himself as a member along with registration of his logo. As stated previously, this is because such registration process bears a meaning as a procedure for registering a

copyright at the authenticate authority. A copyright authentication service for the case of a user's direct embedding of a watermark is also divided into to two cases. One is that both the generation of a logo and the embedment of a watermark are performed by a user. The other is that a logo is generated by the MDCAS and a watermark is embedded by the user.

In the first case, the MDCAS is not involved but a user performs both the generation of the logo and the embedment of the watermark. However, as stated above, even in the case that the user wishes the authentication of a copyright of the original copyrighted material by the certificate authority, the user must register the original, a logo, and data containing the copyright information in the certificate authority. In this case, the user can protect his copyright by the certificate authority by recording information about the entrance and registration dates in the certificate of authority.

In the second case, the client 100 generates his own logo by using the MDCAS server 120 and embeds it into the original copyrighted material, the constitution of which will be explained below with reference to Fig. 2.

Fig. 2 is a block diagram, as an example of a service supplying service according to the preset invention, which illustrates the constitution of a system divided into server/clients sides for providing a watermark embedding service. Unlike the constitution of Fig. 1, the constitution of Fig. 2 additionally includes a logo generation tool 220 enabling a user to generate a logo, and a MDCAS client 210 enabling a client 210 to operate the logo generation tool.

The following is the operation of the above constitution. First, the client 100 accesses the MDCAS server 120 by using a private ID and password given from becoming a member of the MDCAS server 120. A user requests the MDCAS server

120 to generate a logo to be used for his copyrighted material. The server 120 provides a tool for generating a new logo of the client 100, i.e., the logo generation tool 220. The logo generated therefrom is provided to the client 100 via the MDCAS client 210, simultaneously being stored in the database within the DBMS 130.

The client 100 receives the generated logo and then embeds it into the original copyrighted material by using the MDCAS client 210. The MDCAS client 210 existing between the client 100 and MDCAS server 120 is a kind of a virtual system model for a series of operation (watermark embedding operation) to be performed in the client 100. If the client 100 registers the logo in the certificate authority, then the MDCAS server 120 transmits to the client 100 messages as follows: "You should install a plug-in for using a watermark embedding service. Will you install?" If a user selects "YES" in response to this message, a program for the MDCAS client 210 is downloaded from the MDCAS server 120 and then installed in an information processing device of the client 100. If the capacity of the server 120 or its processing speed is excellent and thus there is no concern of extra-loading, it is possible to provide a watermark embedding service in the server without using the MDCAS client program.

Also, in case where a user simply requests the use of copyrighted material stored in the DBMS 130, he should make a request the use of a specific copyrighted material of the MDCAS server 120 without realizing the MDCAS client 210 or logo generation tool 220. Then, the MDCAS 120 embeds the previously registered user information as a watermark by using a watermarking technique of a predetermined method and then transmits the information embedded to the user, i.e., client 100. In this case, the information on the copyrighted material, such as information about a copyright holder and his logo, is embedded as a basic watermark and information about

a user who utilizes such copyrighted material, such as the time that the use of the copyrighted material is requested and personal information about the scope of the use and users, is embedded as a watermark. That is, information about a copyright holder and a user are hierarchically embedded, thereby it is possible to easily grasp a distribution channel of the copyrighted material.

According to another aspect of the present invention, a watermark is extracted from the watermark-embedded copyrighted material to verify and authenticate the copyright information, which is an essential step for a case where an illegal use of the copyrighted material is sensed and thus there arises a dispute between the original copyright holder and an illegal user. When such dispute arises, the certificate authority can authenticate a copyright of the original copyright holder by presenting evidencing materials such as "a certificate of authentication", which contains the registration date and information about a copyright holder and a copyright. At this time, if a user embeds a watermark, both the original data and doubtful data of illegal use are sent to the certificate authority for extracting a watermark embedded in the illegal data. The certificate authority authenticates a copyright after comparing the watermark extracted from the doubtful data with registered individual information and logo data.

In case that copyright information is embedded by the certificate authority, since there exist previously registered individual information and data such as original data and logo in the certificate authority, only the doubtful data of illegal use is sent to the certificate authority. Thereafter, the certificate authority extracts a watermark using the original stored in the database, and then, authenticates a copyright by means of comparison of the doubtful data with the copyright information such as a watermark and logo extracted.

Figs. 3A and 3B are flowcharts illustrating an embodiment of the operation method in a service supplying system according to the present invention. Fig. 3A illustrates a process of embedding a watermark and Fig. 3B illustrates a process of extracting a watermark. The basic flow in the above flowcharts is as follows: First, a user requests an access service of the certificate authority by using his registered private ID. If the ID is not registered, the user should take a step for registering the ID in the certificate authority. The user selects the type of service (copyright information embedment, copyright information extraction) and requests the corresponding service. The server transmits individual user information to DB, confirms it and executes the operation requested. Figs. 3A and 3B are flowcharts, which illustrate in detail the divided user/server sides of the MDCAS process supported on the internet web browser.

First, the process of embedding a watermark of Fig. 3A among the above entire processes will be reviewed. In order to use the copyright authentication service supplying system according to the present invention, a user accesses the internet to access a homepage providing the present service. Then, the user logs in a service system through a login browser which is outputted to the web browser (step 301).

User information is obtained from the database on the database management system 130 based on the user's ID and password inputted during the login process and then determines whether or not the user is registered (step 303). In the case of a new user, he inputs information on his personal information and payment method to be stored as the user information and then goes through the necessary steps to confirm the inputted information (step 305).

If the user is confirmed, the authentication service is begun. In the authentication service, a process of embedding/extracting a watermark and a data format

to be embedded as a watermark (for example, image size) are selected (step 307). If a service selected is a process of extracting a watermark, then it is proceeded to step 330. However, if it is a process of embedding a watermark, then it is checked whether the user is an existing service user (step 313). This is because in the case of an existing user, there exists a user logo previously registered and stored.

In the case of an existing service user, a user logo previously registered and stored in the database is transmitted to the user (step 325). In the case of a new service user, it is checked whether the user has a logo to be used as a watermark (step 315). If he has no logo to be used, a logo is generated by using the logo generation tool 220 provided in the system of the present invention and then a process for storing the generated logo in the client 100 and DBMS 130 is performed (step 317). When a logo is generated, target data in which a watermark is embedded is imported (step 321).

In the embodiment of Fig. 3A, a step of embedding a watermark into the target data is performed by a user (step 323). Concerning the watermark embedding, there may be presumed a case which enables a user to select a watermarking method. For example, in case where each of the watermarking companies (A,B,C) is operated together in the MDCAS server 120, the user may select one method among a variety of watermarking methods. Of course, the operation may be performed in the MDCAS server 120 by providing each watermarking algorithm to the MDCAS server 120 by each company. Otherwise, by operating the watermarking algorithm by each company, each company may perform the watermarking and the MDCAS may purely perform the authentication of the copyright.

In the above case, as illustrated in Fig. 4, the user logs in the MDCAS server 120 and goes through a basic process as mentioned previously. Thereafter, the user

selects one method among a variety of watermarking methods provided by the MDCAS server 120 (step 322), and then, embeds a watermark into data by using the selected watermarking method (step 323). Next, the embedded data and information thereof are stored and managed in the database within the database system 130 (step 326).

The watermark-embedded target data is transmitted back to a server of the certificate authority and the server stores the data received (step 327). Of course, in the step 327, it is judged whether the data to be stored is new data which needs to be newly stored. As a result, if the data is determined to be unnecessary, it is possible to omit them. Next, if a user outputs the watermark-embedded data and information on the watermark (step 329), the process of embedding a watermark is terminated (step 331).

In case that the operation judged from the step 309 is an extraction operation, the operation is performed according to the flow illustrated in Fig. 3B. During the extraction process, an objective data from which a watermark is to be extracted is imported (step 351). The user requests a watermark detection by transmitting the objective data to the server (step 353) and the server begins to perform a watermark detection process (step 355). The server detects whether there exists a watermark embedded during said process (step 357). If a watermark is detected, the watermark is extracted (step 361) and the server transmits user information about the extracted watermark and the extracted data to the user (step 363). However, if a watermark is not detected, a message to the effect that there does not exist a watermark to be extracted is outputted to the user (step 359), and the extraction process is terminated.

Briefly reviewing the foregoing process in which the user can select a watermarking method in connection with the extraction operation, as illustrated in Fig.

4, a user selects a company providing a watermark extraction method in a state that watermarked data are called (step 354). When the watermark extraction method is determined, a watermark is extracted from the corresponding data according to the determined method (step 355), and then, the authentication operation of the data is performed.

Also, in case where a watermark is embedded according to a watermarking method provided by MDCAS, not directly by a user, if it is necessary to authenticate multimedia data, information stored in the above MDCAS is called. Then, a watermark is extracted by using an extraction method of the same company that was selected when a watermark is first embedded. Thereafter, information about a series of copyright and content is authenticated from the extracted information.

Fig. 5 illustrates a method that enables a user to directly embed a watermark and register the watermark-embedded content in MDCAS. In this case, the user does not use the MDCAS but embeds a watermark in the content by a free method and with a product, which the user desires. However, if the user registers the watermark-embedded content in MDCAS for authenticating the content, the user transmits information about the watermarking method used together with the content. That is, such information contains that by what technique and products of which company the watermarking method is performed. The MDCAS stores said information together with the content. If the user requests a series of authentication, then the MDCAS extracts a watermark by selecting a watermark extraction method of each company from said stored information and authenticates it.

In addition, although the flowcharts of Figs. 3A and 3B do not display it, a user's itemized statement for payment is transmitted from the server to the payment

gateway 140 whenever the above watermark embedding/extracting services are performed. Its calculated result is transmitted to the server 120, and again directly to the user 100 or after adding up the total according to a given period.

In summary, the MDCAS server 120 stores, manages and provides data in which copyright information such as information about a copyright holder, the original data, and the copyright holder's logo is embedded. The MDCAS server 120 may also play a role as a provider providing the content.

As noted above, the copyright authentication service of multimedia data is generally explained. Said service is variously applicable according to the kinds of users utilizing such service and the forms of service. Here, the users utilizing the service are copyright holders, copyright authentication users said as sellers who sell copyrighted material, and purchasers who purchase copyrighted materials as authenticated. In this case, during the authenticating process, a user certificate authority (CA) for authenticating a user and a multimedia authentication certificate authority (MACA) for authenticating a copyright of a copyright holder or a seller are involved. All users have their own private keys and receive certificates of authentication enclosing public keys from the user certificate authority (CA).

First, for the case that a copyright holder uses a service according to the present invention, one embodiment of a service process provided to the copyright holder will now be explained. The copyright holder encrypts his original data with his private key. The copyright holder accesses the MACA with his personal ID and requests the copyright authentication of his data. At this time, the copyright holder transmits the encrypted data and a certificate of authentication to the MACA. The MACA first requests the CA to identify the user identity process about the copyright holder.

The CA confirms the data requested and then authenticates a user, i.e., a copyright holder. After authentication, the MACA converts the encrypted data to the original data by using the public key of the transmitted certificate of authentication. The MDCAS server in MACA retrieves a logo and user information previously registered by the user from the database and generates a watermark after organizing the information of the copyright holder retrieved from the database. The copyright information is embedded into the watermark. The logo and personal information (name, identity number, etc.) of the copyright holder transmitted to the server from the database and the logo of other certificate authorities are first embedded into the watermark, and automatically, the date and time information is inserted. Such process is called organization.

A watermark generated in such a method is embedded into the original data. The watermark-embedded data are transmitted to the copyright holder together with the certificate of authentication issued by the MACA. The original data, the generated watermark-embedded data and the copyright information are stored in the database within the DBMS. Further, in case where such process is performed, an itemized payment statement thereof is transmitted to the payment gateway.

In this case, it is possible for the MACA to sometimes play a role as a user certificate authority (CA) .

Next, in case where a user is a content seller, its service process is the same as that of the above process of a copyright holder. Since the seller has a duplication right of a relevant data copyright, he can be considered as being in the position of a copyright holder.

Finally, in case where a user is a content purchaser, the authentication process

between the CA, MACA and user will be explained. First, a purchaser purchases a digital content after accessing a site providing the content. In this case, the site providing the digital content authenticates the purchaser by using encryption algorithm and then provides the content to the authenticated user only. Thus, the content provider plays a role as the CA which authenticates a user. The MACA for a digital data authentication service according to the present invention performs the copyright authentication, operating with a digital content providing site, which performs a user authentication.

In more detail, the content purchaser first accesses the content providing site and is authenticated as a user after going through a registration process such as becoming a member of the site. The content provider, i.e. the CA, transmits to the MACA information about the content requested by the user (kinds of content, etc.), information about the content provider himself, and information about the purchaser. At this time, such information is transmitted in an encryption form.

The MDCAS server in the MACA receives such information and requests information and a logo about the content provider registered in the database of DBMS. The MDCAS server receives the information and logo requested from the database, makes a watermark to be embedded into the original data, and then, embeds the watermark into the original content data. The watermark-embedded data is encrypted again and then transmitted to the CA, i.e., the content provider, together with the certificate of authentication of the MACA. At the same time, the original data, the watermark-embedded data, and the copyright information are stored in the database of MACA.

The content provider transmits to the purchaser the watermark-embedded data

obtained from double-encryption of the received information by using a predetermined encryption method, which is agreed between a provider and purchaser. A right purchaser can obtain his desired content by using a double-encryption key previously provided by the content provider and encrypting the content.

In another embodiment of the present invention, watermark-embedded data may be transmitted directly to a purchaser, not to a content provider.

In such MACA-purchaser-CA (content provider) structure, in case that the MACA plays a role as a content seller, the function of the MACA and CA may be united into a single system.

In a process where the registration and authentication of a copyright using a watermarking system is performed, the present invention uses a new concept named "a copyright certificate authority" as above. The certificate authority is capable of copyright authentication as a third authority. Thus, it may be a single formal authority throughout the world and it may be established from a governmental point of view according to nations. Otherwise, an organization suitable for an establishment standard may be established according to a nongovernmental point of view so as to be authorized by a nation. In any case, since the internet is not confined to a national level but is a network spreaded throughout the whole world, a standard to be commonly used throughout the world is needed. Also, a certificate authority established suitable for such standard is needed and another higher organization is also needed to manage such certificate authority.

As above, in case that the authentication services of the same methods as those of Figs. 4~6 are performed, the different watermarking algorithm from each company may cause problems. As explained previously, since each of the watermarking

methods is quite different from each other in their purposes and methods, it is not easy for the MDCAS to manage them. Thus, in order to settle such problems, the two-layer digital watermarking method is used. This method provides each of the watermarking methods themselves with their own indexes, thereby making it possible to recognize which watermarking method is used and extract again information about a pure copyright and content based on such obtained information, and thus, it is very useful.

Industrial Applicability

As suggested above, the third certificate authority based on a watermarking technique should be established between a digital content provider and a user using the digital content for the following reasons: If both embedding and extracting methods of a watermark are disclosed to the general public, the confidence of copyright authentication would be decreased, and thus the third organization is needed for preventing the general public from performing either of embedding or extracting.

In case where an illegal use of a content is sensed, evidencing the embedment of copyright information by a watermarking system has the following effects: Content owners hope that an embedded watermarking would be a basis for argument of the preservation of his copyright as well as indisputable evidence of his copyright retention. In this case, the original data, copyright holder information, and data about an extracted watermark registered in a certificate authority having public confidence would be indisputable evidence to assert the copyright owner's rights. Thus, in the event that there arise multimedia data copyright-related disputes, such embedded-watermarking would be an influential basis capable of evidencing a copyright of the original copyright holder with respect to data.

Also, in case where each individual performs the embedment and extraction of a watermarking, it is not compelled to impose charges on the performance of embedment and extraction of the watermarking in a general sale of software. However, as suggested in the present invention, if it goes through the third authority, it is easy to impose fixed charges on the performance of use and extraction of a watermark.

The target data into which a watermark is embedded can be extended to data needed for copyright protection or information security such as important digital documents of a company, individual or governmental offices as well as such digital multimedia content. That is, by embedding secret documents or information into the existing multimedia data as a watermark, it is possible to prevent illegal disclosure of information to persons who are not allowed to read them.

The multimedia data copyright authentication authority according to the present invention performs the authentication of a copyright about certain digital copyrighted material as well as is applicable to the transmission/receipt of important documents in the electronic business on the internet. That is, a watermarking technique authenticated by the certificate authority is not confined to the function of simply embedding and extracting information but applicable to data hiding. Thus, if multimedia data such as generally used images or audio data are transmitted after hiding important document content, information, etc. in the same method as a watermarking technique, it is possible to reduce dangerous matters, such as files being illegally stolen, without using an existing encryption transmission method.

While there has been described and illustrated embodiments for multimedia data copyright authentication services according to the present invention, it will be understood to those skilled in the art that all modifications and conversion shall be

limited solely by the scope of the claims appended hereto.

What is claimed is:

1. A service system for supplying a copyrighted material, comprising:

a database for storing information about the copyrighted material; and

a copyrighted material supplying means for providing the copyrighted material, at a user's request through the internet to supply said copyrighted material, wherein said copyrighted material is received from said database and copyright information formed as a watermark is embedded into said copyright material.

2. A service system for supplying a copyrighted material, comprising:

a database for storing information about the copyrighted material; and

a copyrighted material supplying means for providing said copyright material, at a user's request through the internet to supply said copyrighted material, wherein the copyright information received from said database is embedded in a watermark form.

3. The service system for supplying the copyrighted material according to claim 1 or 2, wherein the transmission of data between said copyrighted material supplying means and said user is performed through a web browser.

4. The service system for supplying the copyrighted material according to any one of claims 1 to 3, wherein said watermark is embedded in an image form.

5. The service system for supplying the copyrighted material according to claim 4, wherein said copyright information includes information about a copyright holder and a copyright holder's logo.

6. The service system for supplying the copyrighted material according to claim 4, wherein a type of said watermark to be embedded is selected by said copyright holder.

7. The service system for supplying the copyrighted material according to claim 1, 2, 5 or 6, wherein said watermark is embedded utilizing a two-layer watermarking method.

8. The service system for supplying the copyrighted material according to claim 5 or 6, further comprising a logo generation means for generating a logo capable of indicating said copyright holder, wherein a logo generated by said logo generation means is stored in said database, via said copyrighted material supplying means, as said copyright information.

9. A service system for authenticating a copyrighted material, comprising:

a database for storing information about the copyrighted material; and

a copyrighted material authentication means for performing the authentication of the copyrighted material provided by a user, at said user's request through the internet to authenticate said copyrighted material, wherein a watermark is extracted from the copyrighted material received from said user; the extracted watermark is compared with information about said copyrighted material stored in said database; and the copyrighted material received from said user is authenticated.

10. The service system for authenticating the copyrighted material according to claim 9, wherein the transmission of data between said copyrighted material authentication means and said user is performed through a web browser.

11. The service system for authenticating the copyrighted material according to claim 9 or 10, wherein said watermark is embedded in an image form.

12. The service system for authenticating the copyrighted material according to claim 11, wherein said copyright information includes information about a copyright holder and a copyright holder's logo.

13. The service system for authenticating the copyrighted material according to claim 11, wherein kinds of said watermark to be extracted are selected by said copyright holder.

14. The service system for authenticating copyrighted material according to claim 9, 10, 12, or 13, wherein said watermark is embedded utilizing a two-layer watermarking method.

15. A service method for supplying a copyrighted material, comprising the steps of:

registering a copyrighted material provided by a copyright holder through the internet and copyright information about said copyrighted material;

embedding said copyright information into said copyrighted material as a watermark at a user's request to provide a copyright with respect to said registered copyrighted material; and

providing said watermark-embedded copyrighted material to said user.

16. The service method for supplying the copyrighted material according to claim 15, wherein said watermark is embedded in an image form.

17. The service method for supplying the copyrighted material according to claim 16, wherein said copyright information includes information about a copyright holder and a copyright holder's logo.

18. The service method for supplying the copyrighted material according to claim 17, wherein a type of said watermark to be embedded is selected by said copyright holder.

19. The service method for supplying the copyrighted material according to any one of claims 15 to 18, wherein said watermark is embedded utilizing a two-layer watermarking method.

20. A service method for authenticating a copyrighted material, comprising the steps of:

receiving a copyrighted material at a user or copyright holder's request through the internet to authenticate the copyrighted material;

extracting a watermark from said received copyrighted material; and

transmitting the result of authentication to said user or copyright holder in comparison of the copyright information obtained from said extracted watermark with a stored copyrighted material and copyright information.

21. The service method for authenticating the copyrighted material, according to claim

20, wherein said watermark is embedded in an image form.

22. The service method for authenticating the copyrighted material, according to claim 21, wherein said copyright information includes information about a copyright holder and a copyright holder's logo.

23. The service system for authenticating the copyrighted material according to claim 21, wherein a type of said watermark to be extracted is selected by said copyright holder.

24. The service system for authenticating the copyrighted material according to claim 20, wherein said watermark is embedded utilizing a two-layer watermarking method.

25. A service system for transmitting and authenticating a copyrighted material, comprising:

a copyrighted material provider system which is operated by a provider of copyrighted material;

a database system for storing the copyrighted material provided by said provider of said copyrighted material;

a user system which is operated by a user; and

a server for authenticating the copyrighted material provided by and at a request of said copyrighted material provider and said user, and for providing the copyrighted material,

wherein said copyrighted material provider system is constructed in such a manner that the copyrighted material and copyright-related information for the

copyright authentication are provided to said server so as to be stored in said database system;

said user system is constructed in such a manner that the copyrighted material stored in said database system is selected and displayed at the request of the transmission of a specific copyrighted material; and

said server transmits, respectively, the information about said copyrighted material and the information about said user, which are embedded as watermarks, at a request from said user system to transmit the copyrighted material, and the watermark embedded in said copyrighted material is extracted so as to authenticate a copyright by comparison of the extracted watermark with the copyright-related information stored in said database system at said copyrighted material provider's request or said user's request to authenticate the copyright of the copyrighted material.

FIG 1. 1/6

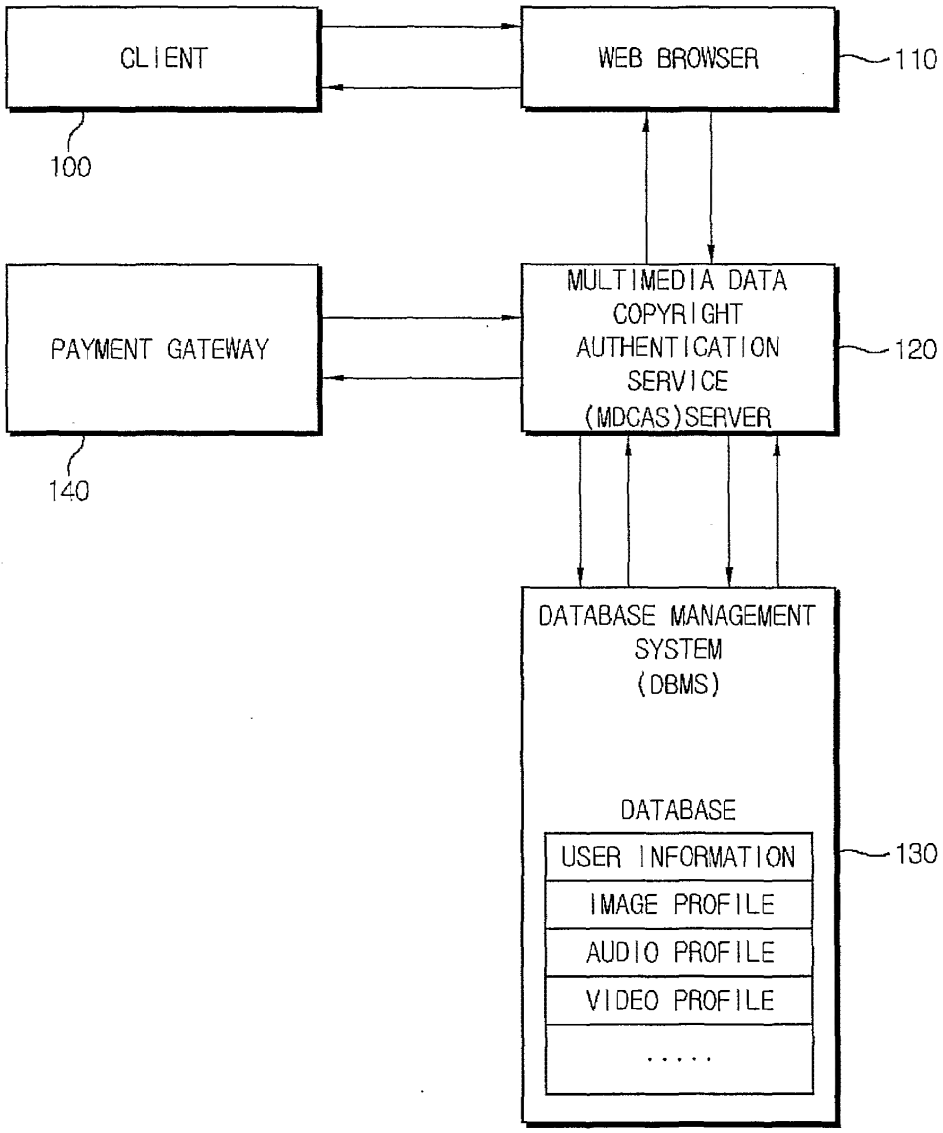

CLIENT
WEB BROWSER
110
100
PAYMENT GATEWAY
MULTIMEDIA DATA
COPYRIGHT
AUTHENTICATION
SERVICE
(MDCAS)SERVER
120
140
DATABASE MANAGEMENT
SYSTEM
(DBMS)
DATABASE
USER INFORMATION
IMAGE PROFILE
AUDIO PROFILE
VIDEO PROFILE
.....
130

FIG 2. 2/6

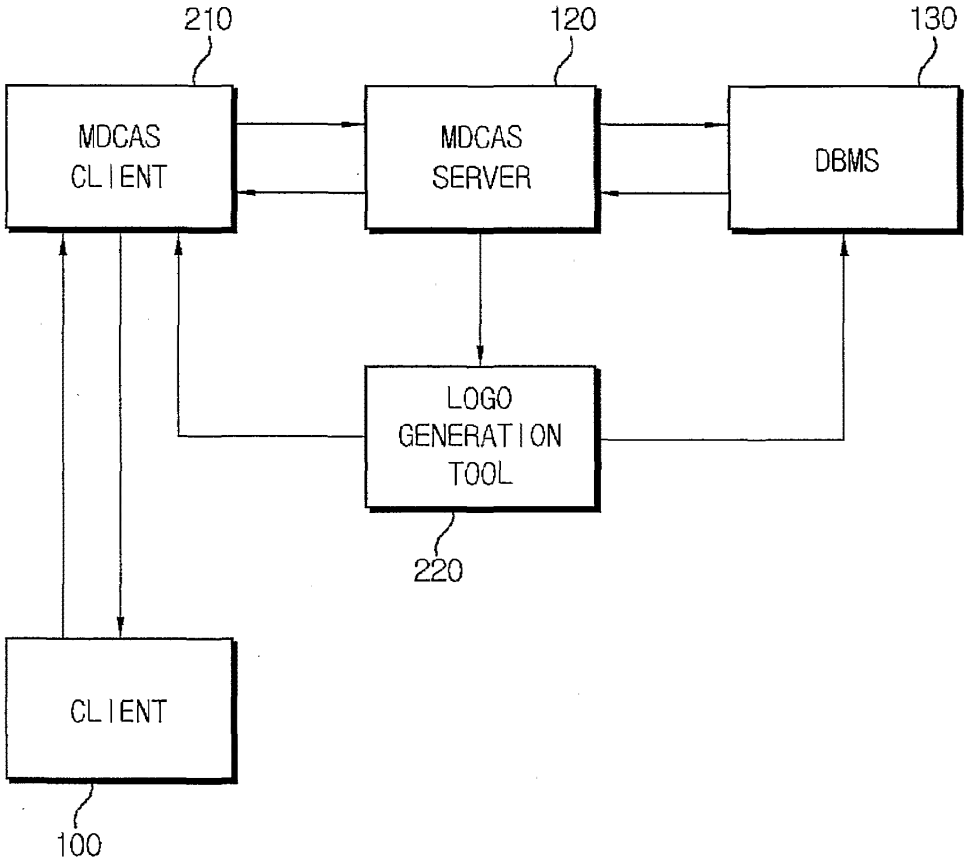

210
120
130
MDCAS CLIENT
MDCAS SERVER
DBMS
LOGO GENERATION TOOL
220
CLIENT
100

FIG 3a. 3/6

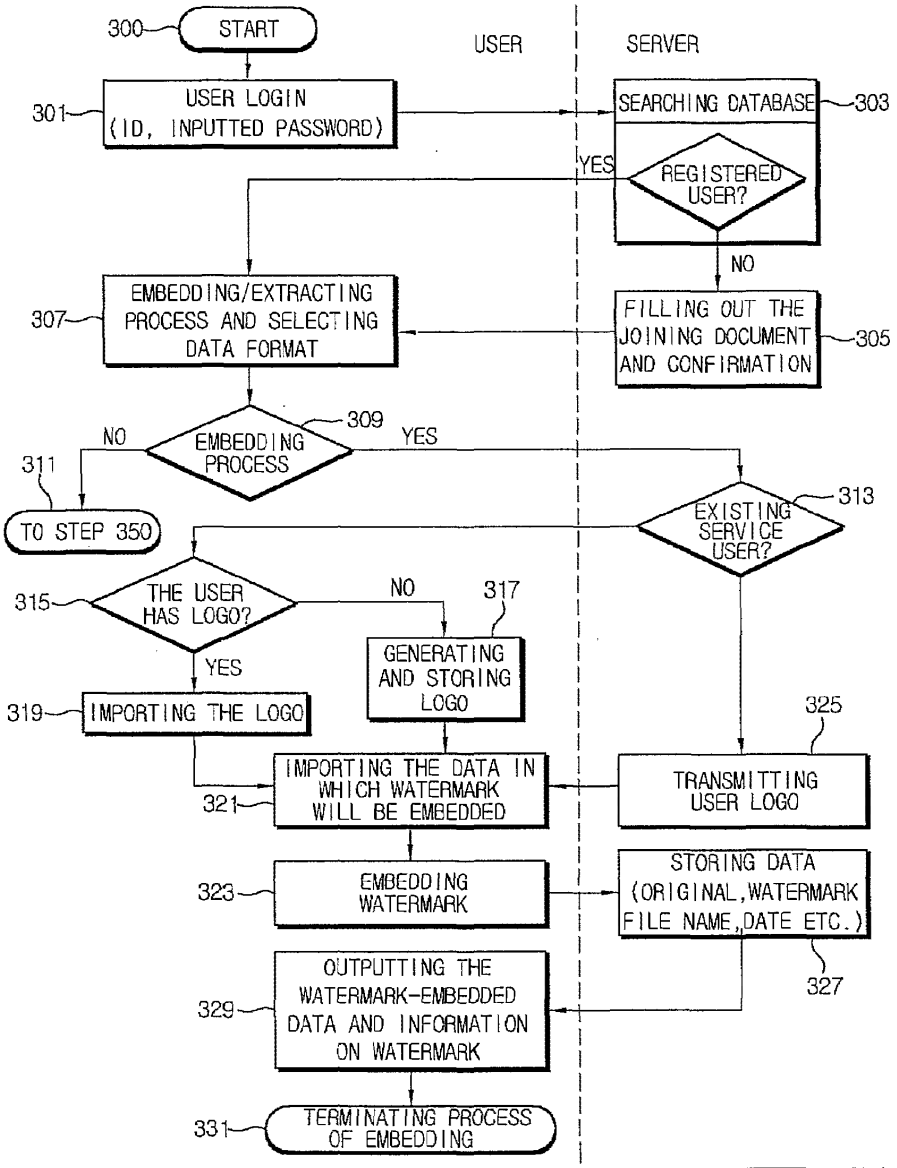

300
START
USER
SERVER
301
USER LOGIN (ID, INPUTTED PASSWORD)
SEARCHING DATABASE
303
YES
REGISTERED USER?
NO
307
EMBEDDING/EXTRACTING PROCESS AND SELECTING DATA FORMAT
FILLING OUT THE JOINING DOCUMENT AND CONFIRMATION
305
309
NO
EMBEDDING PROCESS
YES
311
TO STEP 350
313
EXISTING SERVICE USER?
315
THE USER HAS LOGO?
NO
317
GENERATING AND STORING LOGO
YES
319
IMPORTING THE LOGO
325
IMPORTING THE DATA IN WHICH WATERMARK WILL BE EMBEDDED
321
TRANSMITTING USER LOGO
323
EMBEDDING WATERMARK
STORING DATA (ORIGINAL, WATERMARK FILE NAME, DATE ETC.)
327
329
OUTPUTTING THE WATERMARK-EMBEDDED DATA AND INFORMATION ON WATERMARK
331
TERMINATING PROCESS OF EMBEDDING

FIG 3b. 4/6

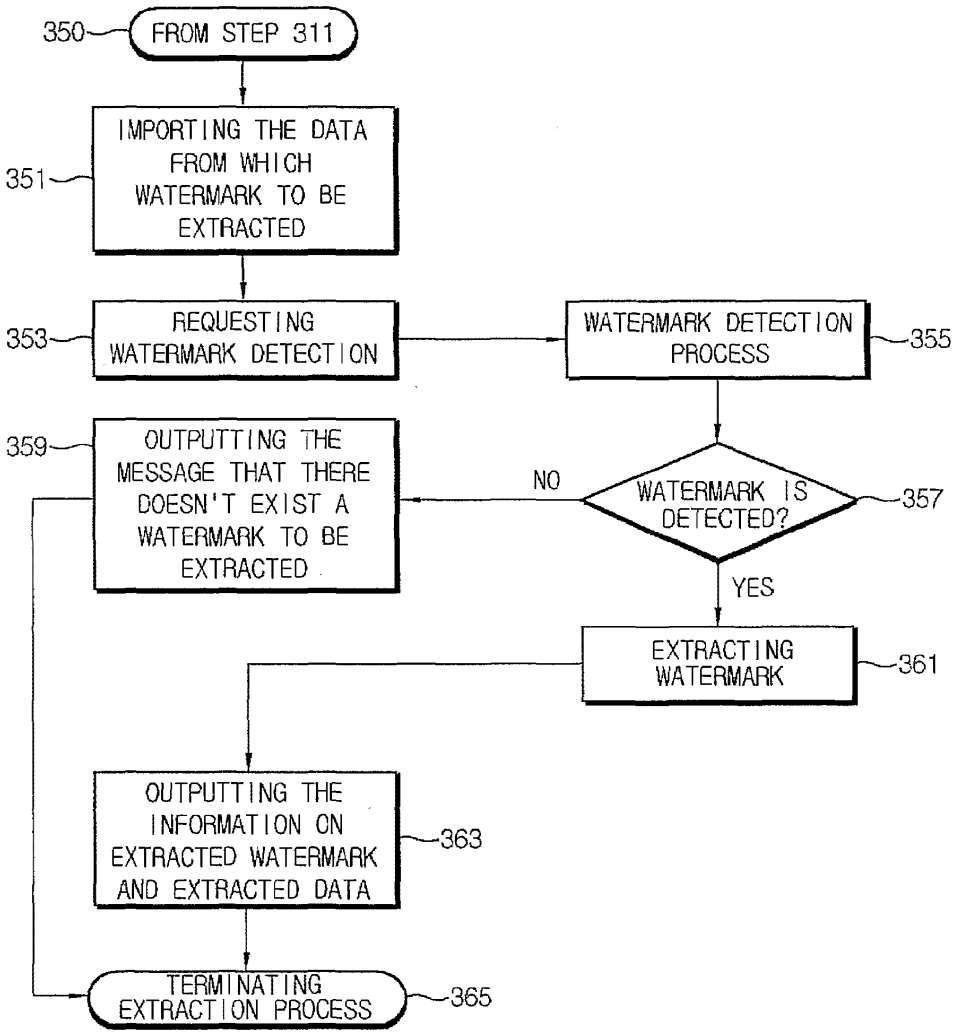

350
FROM STEP 311
IMPORTING THE DATA FROM WHICH WATERMARK TO BE EXTRACTED
351
REQUESTING WATERMARK DETECTION
353
WATERMARK DETECTION PROCESS
355
WATERMARK IS DETECTED?
357
NO
YES
OUTPUTTING THE MESSAGE THAT THERE DOESN'T EXIST A WATERMARK TO BE EXTRACTED
359
EXTRACTING WATERMARK
361
OUTPUTTING THE INFORMATION ON EXTRACTED WATERMARK AND EXTRACTED DATA
363
TERMINATING EXTRACTION PROCESS
365

FIG 4. 5/6

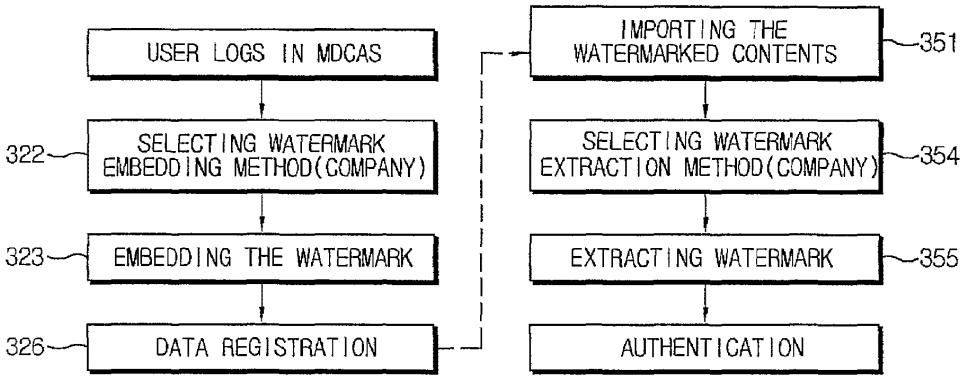
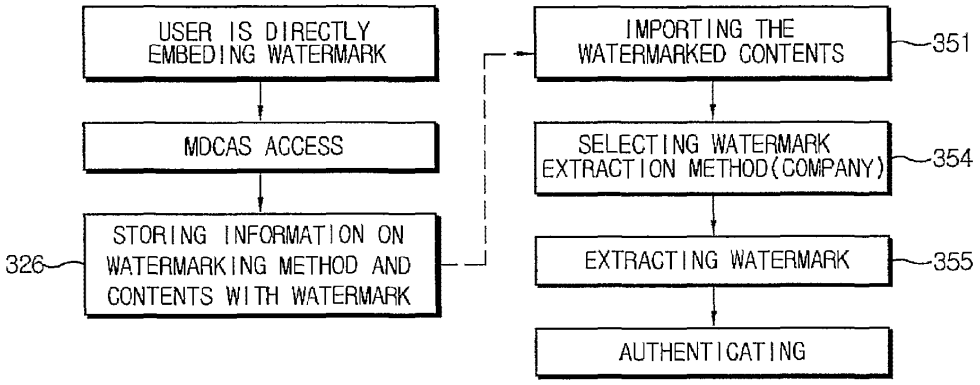

USER LOGS IN MDCAS
322
SELECTING WATERMARK EMBEDDING METHOD(COMPANY)
323
EMBEDDING THE WATERMARK
326
DATA REGISTRATION
IMPORTING THE WATERMARKED CONTENTS
351
SELECTING WATERMARK EXTRACTION METHOD(COMPANY)
354
EXTRACTING WATERMARK
355
AUTHENTICATION

FIG 5. 6/6


USER IS DIRECTLY EMBEDING WATERMARK
MDCAS ACCESS
STORING INFORMATION ON WATERMARKING METHOD AND CONTENTS WITH WATERMARK
326
IMPORTING THE WATERMARKED CONTENTS
351
SELECTING WATERMARK EXTRACTION METHOD(COMPANY)
354
EXTRACTING WATERMARK
355
AUTHENTICATING

INTERNATIONAL SEARCH REPORT

national application No.
PCT/KR01/00997

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 G06F 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimun documentation searched (classification system followed by classification symbols)
G06T 9/00, H04N 5/913, G09C 5/00

Documentation searched other than minimun documentation to the extent that such documents are included in the fileds searched
KR, JP IPC as above

Electronic data base consulted during the internation search (name of data base and, where practicable, search trerms used)
WPI, JPO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5875249 A (INTERNATIONAL BUSINESS MACHINES CO.) 23 FEBRUARY 1999	1-25
Y	KR 1999-82729 A (INTERNATIONAL BUSINESS MACHINES CO.) 25 NOVEMBER 1999	1-25
Y	KR 2000-18052 A (KIM JU HYUN) 6 APRIL 2000	1-25

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevence
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"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
"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
"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevence; 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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 JULY 2001 (30.07.2001)	31 JULY 2001 (31.07.2001)

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, Dunsan-dong, Seo-gu, Daejeon Metropolitan City 302-701, Republic of Korea Facsimile No. 82-42-472-7140	JEON, Hyun Jin Telephone No. 82-42-481-5788

Form PCT/ISA/210 (second sheet) (July 1998)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 February 2002 (07.02.2002)

PCT

(10) International Publication Number
WO 02/11446 A2

(51) International Patent Classification[7]: H04N 7/173

(21) International Application Number: PCT/EP01/07965

(22) International Filing Date: 11 July 2001 (11.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/627,188 27 July 2000 (27.07.2000) US

(71) Applicant: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: **MCGEE, Thomas**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **DIMITROVA, Nevenka**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **AGNIHOTRI, Lalitha**; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **GROENENDAAL, Antonius, W., M.**; Internationaal Octrooibureau B.V., Prof Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: CN, JP, KR.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

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.

WO 02/11446 A2

(54) Title: TRANSCRIPT TRIGGERS FOR VIDEO ENHANCEMENT

(57) Abstract: A system and method for retrieving information supplemental to video programming. Transcript text is searched for terms of interest and information associated with the terms is identified. Depending upon a user profile and the category of video segment being viewed, the supplemental information is formatted for display. Over time, the rules for associating the supplemental information with the terms of interest may be modified using a learning model.

Transcript triggers for video enhancement

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention is directed to the field of media technology. It is particularly directed to video and related transcript text.

2. Cross-Reference to Related Applications

This invention associates video with supplementary information using a text transcript, and extracts and augments textual features, as does co-pending application, Ser Nr. 09/351,086, Filed 1999 July 9 by the assignee, and incorporated by reference herein.

3. Description of the Related Art

In recent years, the number of media sources has increased and the volume of information from each source has also increased, resulting in information overload. Most consumers have neither the time nor the inclination to sift through the morass of information for what is pertinent to their wants and needs. Accordingly, so called "push technology" has developed. Webcasting applications such as Pointcast or Backweb, or the newer web browsers, ask the user which information categories and web sites the user is interested in. A web server then "pushes " information of interest to the user instead of waiting until the user requests it. This is done periodically and in an unobtrusive manner.

Concurrently, as media technology has progressed, the lines between video, audio, and other media have been blurred. Advances in media technology have enabled the delivery of Internet information and other informational material to the consumer's video display, along with the traditional television programming. Because the Internet has become a tool of e-commerce, consumers are conditioned to view a combination of media, video, audio, and text information on the same or associated topics. Consumers are acquainted with the hyperlink concept and the notion of "drilling down" to retrieve additional information on a subject they are viewing on the World Wide Web (WWW).

Retrieval of this additional information can currently be accomplished using closed caption text, audio, and automated story segmentation and identification. The Broadcast News Editor (BNE), provided by Mitre Corporation, enables such retrieval by automatically partitioning newscasts into individual story segments, and providing a

summary of each story segment in the first line of the closed-caption text associated with the segment. Keywords from the closed-caption text or audio are also determined for each story segment.

The Broadcast News Navigator (BNN), also from Mitre Corporation, sorts story segments by the number of keywords in each story segment that match search words selected by the consumer. Accordingly, story segments likely to be of interest to a particular consumer can be readily identified. However, using a combination of BNN and BNE requires that the consumer have an explicit search topic in mind, which is usually not the case in a typical channel-surfing scenario.

Patents which disclose providing the user with information supplemental to a television program include US Patent No. 5,809,471 to Brodsky entitled "Retrieval of additional information not found in interactive TV or telephony signal by application using dynamically extracted vocabulary" and US Patent No. 6,005,565 to Legall et al. entitled "Integrated search of electronic program guide, internet and other information resources." In the '471 patent, keywords are extracted from a television program or closed caption text, creating a dynamically changing dictionary. The user requests information based upon an item seen or word heard in the television broadcast. The user's request is matched against the dictionary, and when there is a match, a search for supplemental information to display is initiated.

In the '565 patent, the user selects topics and sources to search. Based on the user input, the search tool performs a search of the electronic program guide and other information resources such as the World Wide Web, and displays the results. Both the '471 patent and the '565 patent require that the user provide a keyword of interest. Neither patent relates the supplementary information retrieved to the global context of the program, (i.e. news program), as opposed to the subject matter of the program (i.e. the Stock Market report).

SUMMARY OF THE INVENTION

Accordingly, it would be advantageous to provide a method and system employing transcript text, for automatically providing supplementary multimedia information enhancing the consumer's television viewing experience. So called transcript text is comprised of at least one of the following: video text, text generated by speech recognition software, program transcripts, electronic program guide information, and closed caption text that contains all or part of the program information. Video text, is superimposed or overlaid

text displayed in the foreground, with the image as a background. Anchor names for example, often appear as video text. Video text may also take the form of embedded text, for example, a street sign that can be identified and extracted from the video image.

It would also be advantageous to provide supplementary information, which is specific not just to the individual consumer's known interests or profile, but also to the context of the program being viewed. For example, news segments would be associated with links to the Cable Network News (CNN) Web page while commercials would be associated with additional product information. The method and system would use learning models to continually develop new associations between the television content and other media content as well as to customize which type and how much supplementary information should be displayed. In this way, supplementary information would be integrated seamlessly with a television program without disturbing the viewer or requiring any action on the viewer's part.

The present invention addresses the foregoing needs by providing a system, (i.e., a method, an apparatus, and computer-executable process steps), for retrieval of supplementary information associated with a video segment, for display on the consumer's video display. The system includes a recognition engine for determining whether expanded keywords for retrieving supplementary information are contained in the closed captioned text accompanying the video segment or in other transcript related text. If a keyword is found, a stored rule indicates the supplementary information to be displayed, the information having been selected from a larger set of information, and selected in accordance with a user profile and the context of the segment. Alternatively, the transcript keywords are expanded and then matched to the user's profile. The context of the segment is automatically determined based upon classification data. These data include the program classification, object tracking methods, natural language processing of transcript information and/or electronic program guide information.

The information is displayed in a window or superimposed unobtrusively over the main video segment. Alternatively, the information is transmitted, for example to a hand-held device or an email account, stored to secondary storage, or cached in local memory. The system automatically recognizes the beginning and end of each segment, in the story classifications, and so is able to update the subset of rules to correspond to the program segment context.

In a further aspect of the invention, the set of rules for associating supplementary information with the video segment being viewed is dynamic and based upon a learning model. The set of rules is updated from a set of sources, including third-party

sources, and makes information available to the user in accordance with the user's choices and pattern of behavior. In one embodiment, the rules are transmitted from a Personal Digital Assistant (PDA) enabled with a wireless connection.

This brief summary has been provided so that the nature of the invention will be understood quickly. A more complete understanding of the invention is obtained by reference to the following detailed description of the preferred embodiments thereof in connection with the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 depicts a system on which the present invention is implemented.

Figure 2 depicts elements of the processor contained within the system.

Figures 3a and 3b are flow diagrams used for explaining the operation of the present invention.

Figure 4 is a table illustrating supplementary information triggers for a given video segment, according to the present invention.

Figure 4a illustrates how keywords and triggers are expanded.

Figure 5 is a diagram of an embodiment of the invention illustrating a learning model.

Figure 6 is a diagram illustrating how the association rules database, for retrieving supplementary information, is updated and maintained.

Figure 7 is a diagram illustrating how supplementary information is displayed.

Figure 8 is a diagram illustrating one embodiment of the invention in which a set-top box is used.

Figure 9 is a diagram illustrating another embodiment of the invention in which a television display is used.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 shows a representative embodiment of a system on which the present invention is implemented. In this embodiment, a multimedia processor system 6 includes a processor 12, a memory 10, input/output circuitry 8, and other circuitry and components well known to those skilled in the art. An analog video signal or a digital stream is input to the receiver 2. This stream is compliant with MPEG or other proprietary broadcast formats.

In accordance with the MPEG standard, video data is encoded using discrete cosine transform encoding and is arranged into variable length encoded data packets for

transmission. One version of the MPEG standard, MPEG-2 is described in the International Standards Organization — Moving Pictures Experts Group Document "Coding of Moving Pictures and Audio", ISO/IEC JTCI/SC29/WG11, July, 1996. MPEG is just one example of a format, which can be utilized in the system.

Transcript text, transmitted in the video signal 162, is extracted by the transcript extractor 4 from either line 21 of the analog video signal or the user data field of the MPEG stream. The transcript extractor 4 also partitions the video program into segments. The transcript text for the particular frame may be stored in the memory 10. Alternatively, it is analyzed as a real-time data stream.

Also stored in the memory 10 is Electronic Program Guide Information (EPG). This information, describing television broadcast information for a period of days or weeks, is downloaded on user request or at a preprogrammed time. It is transmitted by local analog TV broadcasters over the vertical blanking interval or through MPEG-2 private tables on a "home barker" channel. It can also be transmitted via telephone line or through wireless means. EPG data includes information such as the program's genre and subgenre, its rating, and a short program description. EPG data is used to determine the context of a program, such as whether it is a news program, a paid programming excerpt, a soap opera, or a travelogue.

Also stored in secondary storage 18 and available in the memory 10 is personal profile information, in the form of keywords or "triggers," describing the user's interests. Typical triggers could be "Clint Eastwood", "environment", "presidential election" or "hockey". These triggers are expanded in one aspect of the invention to include synonymous and related terms.

As is well known in the prior art, a personal profile of the user's interests is established automatically, by user input, or by a combination of both methods. For example, the TiVo™ Personal TV Service allows the user to indicate which programs the user prefers using a "Thumbs Up" or "Thumbs Down" button on the TiVo™ remote. TiVo™ then builds upon this information to select other related programs the user likes to view.

When a trigger matches keywords contained in the transcript text, supplementary data is retrieved, for example from the Internet 14 or proprietary sources 13 through the communication means 17. Another source for supplementary data is, for example, another channel. The data is then displayed to the user on a display 16 either as a Web page or a portion thereof or superimposed over the main video in a non-intrusive

fashion. Alternatively or additionally, a simple Uniform Resource Locator (URL) or informative message is returned to the viewer.

Rules for associating these triggers with supplementary data such as World Wide Web (WWW) pages are also stored in the secondary memory 18 and available from the memory 10. These rules are established through a default profile that is updated based on user behavior, or though a query program that prompts the user for interests and then generates the rule set. The rules are also received from a mobile device 15 such as a Personal Digital Assistant (PDA) or cell phone through the communications means 17. These rules associate supplementary information with the triggers, depending on the context of the program segment being viewed. For example, if a program segment is an advertisement for Clint Eastwood's new movie, the context is commercial and the supplementary data retrieved is a description of the movie he is starring in. If a program segment is a description of Clint Eastwood's car accident, the context is news, and the supplementary data retrieved is a biographical web page or a link to www.cnn.com to obtain more information about why he is in the news.

As illustrated above, association rules are also dependent upon a combination of EPG fields. For example, if "Clint Eastwood" appears in the actor's field of the EPG data, and the context is determined to be commercial, and the closed caption data is "We will be returning shortly to Clint Eastwood and Fist Full of Dollars after these announcements," then, the association rule retrieves supplementary data pertaining to the particular movie being shown. On the other hand, if "Clint Eastwood" does not appear in the actor's field of the EPG data, and the context is commercial, and the closed caption data is "High Plains Drifter starring Clint Eastwood will be aired on Friday," then, the association rule retrieves supplementary data pertaining to showtimes for the movie. These differences can be determined, for example, by comparing the text of the credits with text extracted from the closed caption data. It there is a match, then the program being advertised is the program being viewed. Alternatively, natural language processing can be used to identify key phrases such as "returning to" which would also indicate that the program being advertised is the program being viewed.

Alternatively, if "Clint Eastwood" does not appear in the actor's field of the EPG data, and the context is commercial, and the closed caption data says "Clint Eastwood's new movie will be released shortly", then the association rule retrieves supplementary data by linking to the Clint Eastwood home page to find out more about the movie.

Association rules also determine the category of media to be retrieved. For example, if "Kosovo" is the trigger and the program is sponsored by National Geographic, the association rule retrieves a map of the region. Alternatively, if the program segment context is news and the word "war" is located in the EPG data, then the association rule retrieves a recent political history of the region.

In alternative embodiments, the system includes a video display with built-in processing and memory, or a separate set top box for processing and storing information. These embodiments can include communication means or interface to communication means. Receipt of the video signal and Internet information is via wireless, satellite, cable or other media. This system is modifiable to transmit the supplementary information via the communication means 17 as an output signal over a radio transmitter, or via wireless means, where the signal is embodied in a carrier wave 160. The supplementary information is transmittable to an e-mail list, and/or downloadable to the voice mail feature of mobile devices 15 such as cell phones and/or transmittable to a hand held device such as the Palm Pilot®.

Figure 2 is a diagram of the processor elements. A profile generator 50 generates and stores a profile of the user's known interests, which includes trigger information or keywords of interest. This is accomplished for example through user input, by having the user respond to a series of queries, by creating a default profile based on user characteristics which are modified by the user, or by monitoring user activity to discover areas of interest. The rule generator 52 generates the association rules which logically combine each trigger with a variety of contexts to determine which supplementary information should be displayed to the user. The recognition engine 54 compares each trigger with the transcript text and determines whether the trigger exists as a keyword in the text. When a trigger is matched, the retrieving portion 56 retrieves the supplementary information and the formatting portion 58, formats the data for display. The context monitor 60, monitors the context to see whether it is changing due to the display of a new program segment. When a context change occurs, the context monitor 60 accesses the secondary storage 18 to retrieve a new subset of association rules.

The data updater 62 is used to update the supplementary information to incorporate new web sites, for example, or to reflect the results of searches performed by various search engines. The repetition counter 64 counts the frequency with which a particular piece of information is requested and the clickstream monitor 66 measures the frequency with which a user requests supplementary data in general. These intelligent agents

work in conjunction with the retrieval modifier 68 to modify the type of information and amount of information presented to the user.

Figures 3a and 3b are flow diagrams illustrating the method of the invention. To begin, in step S201, the input video is input to a receiver. The video is in analog or digital form. The transcript extractor, which is separate from or incorporated into the processor, extracts the transcript text in step S202 and identifies the beginning and end of each video segment. Next, in step S203, the processor retrieves the keywords from the transcript text. Extraction of keywords is well known in the art and one such method of extraction is described in U.S. Patent No.5,809,471 to Brodsky, entitled "Retrieval of additional information not found in interactive TV or telephony signal by application using dynamically extracted vocabulary." As shown in Figure 4a, these keywords 152 are extracted from the transcript text 150 and expanded 154 to achieve more meaningful and complete results, by associating them with synonymous or related keywords as shown in Figure 3a step S204. A thesaurus is used for this purpose or a database such as Wordnet®. Wordnet® is an on-line lexical reference system whose design is inspired by current psycholinguistic theories. The various parts of speech are organized into synonym sets, each representing one underlying lexical concept.

Keywords can also be expanded by identifying the theme of the transcript text. For example, the presence of the trigger "economy" in transcript text can be derived, when a number of words such as "inflation", "Alan Greenspan", and "unemployment rate" are simultaneously present. Similarly, the presence of the trigger "President Clinton" can be derived if the keyword "President of the United States" is present in the transcript text.

Special rules apply when the supplementary data is contained in reference tools such as dictionaries and encyclopedias, as shown in Figure 4 114 132. In one mode, triggers are mapped to a variety of keywords depending on the level of understanding of the viewer. For example, if the viewer is a child or foreign-speaking viewer, the trigger "unemployment" would be mapped to the keyword phrase "without a job" but would not be mapped to the keyword "redundancy." In an alternate mode, the keywords are expanded as described above.

Parental control is implemented below the program level at the program segment or contextual level. Therefore, parents need not worry if a commercial inappropriate for children is shown during an otherwise appropriate cartoon show, for example. The child viewer is presented with a special screen only during the commercial. This special screen may take the form of a toy advertisement instead of merely a typical blocking screen.

Blocking triggers are also expanded to enhance the effectiveness of the blocking. For example, if the parent does not want the child to see video segments related to war, the trigger "war" is mapped to keywords and phrases such as "armed conflict" and "bombing." An example of trigger expansion is shown in Figure 4a 102 156.

Returning to Figure 3a, in step S205, the personal profile containing the triggers is read. The processor matches the keywords developed from the transcript text with the triggers contained in the user profile in step S206. If there is no match, the processor continues by extracting additional transcript text.

If there is a match, in step S207 of Fig. 3b, the context of the ongoing video program is identified. This is done in several ways, using either the closed caption data, EPG data, object tracking methods, or low-level feature extraction such as color, motion, texture, or shape. The context of the program segment is also extracted from the transcript text using natural language techniques. For example, Microsoft Corporation has developed software that learns by analyzing existing texts, including online dictionaries and encyclopedias, and automatically acquiring knowledge from this analysis. This knowledge is then used to help constrain the interpretation of the word "plane" in a sentence like "Flying planes can be dangerous" and to determine that the sentence pertains to aviation rather than woodworking.

Software also operates at the discourse level, using discourse analysis to identify the structure of the closed caption text and thereby its context. For example, a news program is identified because it would generally report the most important facts, "who, what, when, where, how" in its beginning. Accordingly, a program that began with the sentence "Clint Eastwood was in a gun fight, in Carmel California, at seven a.m. on Main Street, by a bystander with a home video camera" is identified as a news story. The context is also available in the EPG data from the genre and sub genre fields or a combination of fields as explained above.

Next, in step S208, the association rules are read. The association rules determine which supplementary data from a stored database should be retrieved, based upon the keyword and context. In step S209, the customized display modules are read. These modules enable the user to restrict the types of information, and therefore also the amount of information, the user wants to view. For example, the user may only wish to see the Uniform Resource Locator (URL) of a WWW page, only larger titles from the page, a page summary, or a full page. The user can choose the supplementary sources he wants to view and prioritize these sources.

In step S210, the supplementary data is retrieved from a database stored in memory. The database contains items of interest or pointers to items of interest, ancillary to the trigger. For example, the database contains any of the following: names of celebrities and public figures, geographic information such as countries, capitals, and presidents, product and brand names, assorted categories and topics.

The database is maintained and refreshed from an established set of sources. These include for example, the Bloomberg site, encyclopedias, thesauri, dictionaries, and a set of web sites or search engines. Information from the EPG and closed caption data is also incorporated into the database.

A set of refresh and cleanup rules, as shown in Figures 5 and 6 is also stored in a database or a viewer's profile, for example, and maintained for managing the size of the database or profile and its currency. For example, "stale" items such as election results and links to information about polls and the candidates would be deleted after an election takes place.

Returning to Figure 3b, in step S211, the supplementary information is formatted for display. The information is displayed in a window or superimposed unobtrusively over the main video segment. Alternatively, the information is formatted for transmittal, for example to a hand-held device such as the Palm Pilot™ distributed by Palm, Inc. or to an email account.

Figure 4 illustrates the set of association rules 100 for several triggers 102. In the table, the first column represents the triggers 102 and columns 2-4 represent the possible contexts 104, 106, 108, 110 for the example triggers shown. Beginning with the association rule 120 for the first trigger 102, "Clint Eastwood", when this trigger 102 appears in a user's profile, one of three different items of supplementary information 116, 118, 120 are retrieved for display, depending on the context in which Clint Eastwood appears in the video segment being viewed. Although only one link is shown in each box of the example table, multiple links can exist. If Clint Eastwood appears in a commercial, the system will link to the WWW page located at www.imdb.com and display the page in accordance with the customized display model. If Clint Eastwood appears on a talk show, the talk show segment where he appears will be stored for retrieval 118 and/or an alert sent to the viewer in real-time. Alternatively, an offline alert is transmitted for later viewing, notifying the viewer that the segment has been stored.

Alerts are automatically or manually retrieved. Alert transmission is also keyed to a topic such that the alert is displayed the next time a Clint Eastwood movie is

shown. If Clint Eastwood appears on a news program, the system will link to the WWW page located at www.cnn.com. Alerts have priorities enabling the user to select the circumstances when the user wants to be notified. For example, a user may only want to view alerts pertaining to severe weather warnings.

The second association rule 122 for the trigger 102 Macedonia deals with 4 different contexts. If the trigger "Macedonia" appears in an advertisement, the system links to the WWW page at www.travel.com 130. If Macedonia is the subject of a talk show, the system links to an entry for "Macedonia" in Compton's Encyclopedia 132. If Macedonia is the subject of a news show, the user is tuned to the station where the program is being aired 134. If Macedonia is the subject of a program sponsored by National Geographic magazine, the system links to www.yahoo.com/maps 136 to display a map of Macedonia.

Association rules 3-5 124 126 128 should be interpreted in the same manner as the above examples. As shown in the table, when certain triggers 102 such as "Meryl Streep" appear in transcript text, the system will only provide supplementary information for certain contexts. In the case of "Meryl Streep", supplementary information is only supplied for the Talk Show and News contexts. If desired, such a rule is broadened to apply to a list of well-known actors or all actors.

Figure 4a illustrates how both the triggers and keywords can be expanded to retrieve supplementary information. For the example transcript text 150 shown, the keyword 152 "Lyme Disease" is extracted from the transcript text 150. The keyword 152 is then expanded to map to the additional key words "tick", "tick bite", "bull's eye rash" and "deer tick." If any of these expanded keywords appear in the transcript text, supplementary information related to Lyme Disease will be retrieved.

Figure 4a also illustrates how triggers are expanded. The trigger 102 "Lyme Disease" is expanded 156 to include the related terms "tick bite", "West Nile virus, and "mosquito spraying." Accordingly, if the transcript text 150 contains any of the expanded triggers the segment is stored, for example.

Figure 5 illustrates how a learning model is implemented to continually update the customized display modules and association rules. The repetition counter 20 maintains a count of how often the user requests the same supplementary data, for example by clicking on a URL. Also, more than one piece of supplementary information may be retrieved by the retrieving portion 56 of the processor, shown in Figure 2, for each segment and the user may select the information the user wishes to view. If a user requests a particular piece of supplementary data less than a predetermined amount of times, the stored association rules 26

are updated by the retrieval modifier 24 such that the supplementary data is eliminated from the rule or the rule is modified to include a new source. The clickstream monitor 22 monitors how frequently the user requests any supplementary data. If the user selects supplementary data less than a predetermined amount of times, the custom display module 28 for that user is modified by the retrieval modifier 24 such that less information is presented to the user.

Figure 6 illustrates how the dynamic association rules database is updated and maintained. The database contains items of interest or pointers to items of interest that can provide ancillary information, when triggered by a match between a keyword in the transcript text and a trigger in the user's profile. The database is updated over time to reflect current events and to match the evolving user profile.

The existing data sources set 36, specifies the data sources from which the association rules database 26 is constructed. The data sources set 36 which includes both external data 38 from a variety of published sources, proprietary information, and data from the Internet 14 is updated by the data updater 40 to incorporate new web sites, for example, or to reflect the results of searches performed by various search engines. A set of refresh rules 32 is maintained to keep the size of the database at a preset limit. According to a set of established priorities, information is deleted when necessary. A set of cleanup rules 34 is also maintained which specify when and how "stale" information can be deleted. Information in certain categories is date stamped, and information older than a preset number of months and/or years is deleted.

Figure 7 illustrates an embodiment in which the supplementary information 70 is displayed superimposed unobtrusively over the main video segment. The supplementary information appears at the bottom of the picture.

Figure 8 illustrates an embodiment in which a set-top box 75 comprises a receiver 2, which receives video program and transcript text. A transcript text extractor and segmenter 4 extracts the transcript text 150 from the video signal and associates it with segments of the video program such as commercials and news flashes. A processor system 6 includes processing elements well known in the art -- an input/output portion 8, a memory 10, and a processor 12. Via a communication means 17, the processor system retrieves information supplemental to the video program from a variety of sources. Three of these sources, the Internet 14, proprietary (non-public) databases 13, and mobile devices 15 such as PDAs are shown in the figure as examples. The communication means 17 can connect to other devices not specifically shown, via wireless means, cable modem, a digital subscriber line, or a network, for example. The secondary storage 18 is used to store the supplementary

information as well as the rules for retrieving the information. The set-top box can be interfaced to a display such as a PC display or a television.

Figure 9 illustrates another embodiment in which a television 80 comprises a receiver 2, a transcript text extractor and segmenter 4, a processor system 6, secondary storage 18, a communication means 17, and a display 16. The processor system 6 includes processing elements well known in the art - - an input/output portion 8, a memory 10, and a processor 12. The television 80 interfaces to sources of supplementary information via the communication means 17 which interfaces to the Internet 14, proprietary sources 13 and mobile devices 15, for example.

The present invention has been described with respect to particular illustrative embodiments. It is to be understood that the invention is not limited to the above-described embodiments and modifications thereto, and that various changes and modifications may be made by those of ordinary skill in the art without departing from the spirit and scope of the appended claims.

CLAIMS:

1. An association method for retrieving information supplemental to a video program comprising the steps of:

receiving the video program (2);

identifying in the video program at least one segment (4);

receiving classification data for said at least one segment (4,2);

receiving transcript text for the video program (4);

identifying a user profile for a video program viewer (50);

identifying a set of rules (52) incorporating the classification data, for associating the supplementary information with the video program, when the transcript text and the user profile satisfy a set of conditions; and

automatically retrieving the supplementary information based upon the set of rules for display on a display (56).

2. The method according to Claim 1, wherein the set of rules (100) includes information from the user profile (102).

3. The method according to Claim 2, wherein the user profile contains at least one trigger (102) which identifies a topic of interest to the video program viewer.

4. A method according to Claim 3, wherein the set of conditions specifies that a recognition engine (54) retrieve the supplementary information only when a keyword in the transcript text matches (S206) the at least one trigger (102) in the user profile.

5. The method according to Claim 1, wherein the transcript text is comprised of closed caption text, video text, program transcripts or electronic program guide information.

6. The method according to Claim 1, wherein the transcript text (150) is generated by speech recognition software.

7. The method according to Claim 1, further including the step of receiving at least a portion of the set of rules (100) from a mobile device (15) or a third-party source (13).

8. The method according to Claim 1, wherein at least part of the supplementary information and pointers to the supplementary information are stored in a database (26) or transmitted to a personal digital assistant (15) or to an electronic mail address (14).

9. The method according to Claim 1 wherein the retrieval of the supplementary information (116,118,120) is in real-time.

10. The method according to Claim 1, wherein the supplementary information (116,118,120) is formatted for display in a window (70) or for superimposition over the video program on a display (16).

11. The method according to Claim 1, wherein the supplementary information is text information (114) or a page from the World Wide Web (116).

12. The method according to Claim 5, further including the step of automatically selecting the set of rules (100) for each video program segment from the electronic program guide information (150).

13. The method according to Claim 3, further including the step of automatically selecting the set of rules (100) by applying natural language processing to the transcript text (150) for each video program segment to identify whether a keyword (S203) in the transcript text (4) matches a trigger (102) in the user profile.

14. The method according to Claim 3, further including the step of identifying at least one keyword (S203, 152) in the transcript text (150), expanding the at least one keyword (S204, 152) to include related terms (154), and retrieving the supplementary information (S210) when the keyword or related terms matches (S206) the at least one trigger (102) in the user profile.

15. The method according to Claim 3, further including the step of automatically generating the set of rules (52) by applying discourse analysis to the transcript text (150) for

each video program segment to identify whether a keyword (152) in the transcript text (150) matches a trigger (S206,102) in the user profile.

16. The method according to Claim 3, further including the step of expanding at least one trigger (154) in the user profile to include related terms, identifying at least one keyword in the transcript text, and retrieving the supplementary information when the trigger or related terms matches the at least one keyword in the transcript text.

17. The method according to Claim 8, further including the step of deleting (40) supplementary information (26) or pointers to supplementary information added to the database before a certain date or related to events that have terminated.

18. The method according to Claim 11, wherein only the Uniform Resource Locator (URL) (28,70) of the page or wherein a portion of the page (28) which is less than the entire page or wherein a summary of the page (28) is displayed.

19. The method according to Claim 1, further including the step of monitoring (22) the amount of supplementary information viewed by the video program viewer, and the frequency (20) with which the video program viewer views the supplementary information, and varying (24) the amount of supplementary information formatted for display correspondingly, according to a predetermined formula.

20. The method according to Claim 1, wherein the supplemental information is included in an electronic mail message (15) or is downloaded (17) to a personal information manager (15).

21. An apparatus for retrieving information supplementary to a video program, the apparatus comprising:

a receiver (2) which receives the video program, classification data for the video program, and transcript text for the video program;

a transcript extractor (4) which identifies at least one segment within the video program and associates transcript text with said one segment;

a context monitor (60,S207), which monitors the classification data (104,106,108,110) for each segment thereby identifying a context for each segment;

a profile generator (50), which establishes a user profile for a video program viewer;

a rule generator (52), incorporating the classification data (102,104,106,108,110), which establishes a set of rules (100) for associating supplementary information (116,118,120) with the video program, when the transcript text (150) and the user profile (102) satisfy a set of conditions;

a retrieving portion (56), which retrieves the supplementary information (116,118,120), based upon the set of rules (100);

a formatting portion (58) which formats (S211) the retrieved supplementary information for display along with the video program.

22. An apparatus according to Claim 21 wherein the retrieving portion retrieves (S210) the supplementary information (116,118,120) when a trigger (102) within the user profile matches (S206) a keyword (152) within the transcript text.

23. An apparatus according to Claim 22, wherein at least one trigger (102) in the user profile is expanded (156) to include related terms and the trigger and the related terms are compared (S206) with the keyword (152).

24. An apparatus according to Claim 22, wherein at least one keyword (152) within the transcript text (150) is expanded (154, S204) to include related terms and the trigger (102) is compared with the keyword (154) and the related terms.

25. An apparatus according to Claim 21, wherein the retrieving (S207, 104,106,108,110) portion (56) retrieves information for the segment based upon the context of the segment.

26. Computer-executable process steps to retrieve information supplemental to a video program, the computer-executable process steps being stored on a computer-readable medium (18) and comprising:

a receiving step (S201) to receive the video program, classification data describing the video program, and transcript text for the video program;

a context identifying step (S207) to identify at least one segment in the video program and the context of the segment based upon the classification data;

a keyword identification step (S203) to identify keywords in the transcript text for the at least one segment in the video program;

a keyword expanding step (S204) to expand the keywords to include related terms;

a personal profile retrieving step (S205) to retrieve a user profile for a viewer viewing the video program;

a keyword matching step (S206) to match the keywords and the related terms with the at least one trigger in the user profile;

an association rules retrieving step (S208) to retrieve a set of rules specifying which information supplemental to the video program will be retrieved, depending upon the identified context;

a retrieving step (S210) to retrieve the supplementary information based upon the set of rules when the keyword matching step is successful; and

a formatting step (S211) to format the retrieved supplementary information for display;

27. A signal (160), embodied in a carrier wave, representing a video program (162) and information supplemental thereto (116,118,120), comprising video program classification data (104,106,108,110); transcript text (150); a user profile (102); and rules (100) incorporating the video program classification data, for associating the supplementary information with the video program when the transcript text and the user profile satisfy a set of conditions (S206).

28. An apparatus for retrieving and displaying information supplemental to a video program comprising:

means (2) for receiving the video program (162);

means for identifying in the video program at least one segment (4);

means for receiving program classification data describing the at least one segment (4,2);

means for receiving transcript text (150) for the video program and associating the transcript text with the at least one segment (4);

means for retrieving a user profile for a video program viewer (50);

means for identifying (52) a set of rules (100), incorporating the classification data (104,106,108,110), for associating the supplementary information (116,118,120) with

the video program, when the transcript text and the user profile (102) satisfy a set of conditions (S206);

means for retrieving the supplementary information based upon the set of rules (56,S210); and

means for formatting (58) the supplementary information for display along with the video program.

29. A set-top box (75) for a video program viewer, comprising:

receiving means (2) which receives a video program (102), classification data for the video program (104,106,108,110), and transcript text (150) for the video program;

transcript text extraction and segmenting means (4) which identifies at least one segment in the video program and associates transcript text with the at least one segment;

communication means (17) which connects to at least one information source (14,13,15) and receives information supplemental to the video program (116,118,120);

processor means (6) which

a) retrieves a user profile (50) for the video program viewer which contains at least one trigger (102) reflecting an interest of the video program viewer,

b) associates the classification data with the at least one segment (60, S207),

c) identifiifes a set of rules (52) incorporating the classification data, for associating the supplemental information with the segment,

d) searches the transcript text for a trigger contained in the user profile (54),

e) retrieves the supplemental information (56), using the communication means (17) and based upon the set of rules (100), when the trigger (102) is contained within the transcript text (150), and

f) formats (58) the retrieved supplemental information for display; and

storage means (18) which stores the transcript text, the user profile, the set of rules, and the supplemental information.

30. The set-top box (75) according to Claim 29, wherein the receiving means receives a digital video program.

31. The set-top box according to Claim 29 (75), wherein the processor (12) decodes and formats the digital video program for display on an analog display.

32. The set-top box (75) according to Claim 29, wherein the video program viewer selects a destination (15) where the supplementary information will be transmitted via the communication means (17).

33. The set-top box (75) according to Claim 29, wherein more than one type of supplementary information (116,118,120) is retrieved by the processor (12) for each segment, the retrieved supplementary information is automatically placed in an order of priority according to the user profile (S209), and the supplementary information with highest priority is formatted for display (S211) by default.

34. The set-top box (75) according to Claim 29, wherein more than one type of supplementary information (116,118,120) is retrieved by the processor (12) for each segment, and the video program viewer selects the retrieved supplementary information the video program viewer wishes to view.

35. A television set (80) comprising:

receiving means (2) which receives a video program (162), classification data for the video program (104,106,108,110), and transcript text (150) for the video program;

transcript text extraction and segmenting means (4) which identifies at least one segment in the video program and associates transcript text with the at least one segment;

communication means (17) which connects to at least one information source and receives information supplemental to the video program;

processor means (12) which

a) retrieves a user profile (50) for a video program viewer which contains at least one trigger reflecting an interest of the video program viewer,

b) associates the classification data with the at least one segment (4,2),

c) identifies a set (52) of rules (100), incorporating the classification data, for associating the supplemental information with the segment,

d) searches the transcript text (54) for a trigger (102) contained in the user profile,

e) retrieves the supplemental information (116,118,120), using the communication means (17), and based upon the set of rules (100), when the trigger (102) is contained within the transcript text, and

f) formats (58) the retrieved supplemental information for display;

storage means (18) which stores the transcript text, the user profile, the set of rules, and the supplemental information; and

display means which displays the video program and the retrieved and formatted supplemental information.

36. Computer-executable process steps to retrieve information supplemental to a video program, the computer-executable process steps being stored on a computer-readable medium (18) and comprising:

a receiving step (S201) for receiving the video program, classification data describing the video program and transcript data for the video program;

a segmenting step (S202) for identifying at least one segment in the video program and classification data for the segment;

a first identifying step (S205) for identifying a user profile for a video program viewer;

a second identifying step (S208) for identifying a set of rules incorporating the classification data, for associating the supplementary information with the video program, when the transcript text and the user profile satisfy a set of conditions; and

a retrieving step (S210) for automatically retrieving the supplementary information based upon the set of rules.

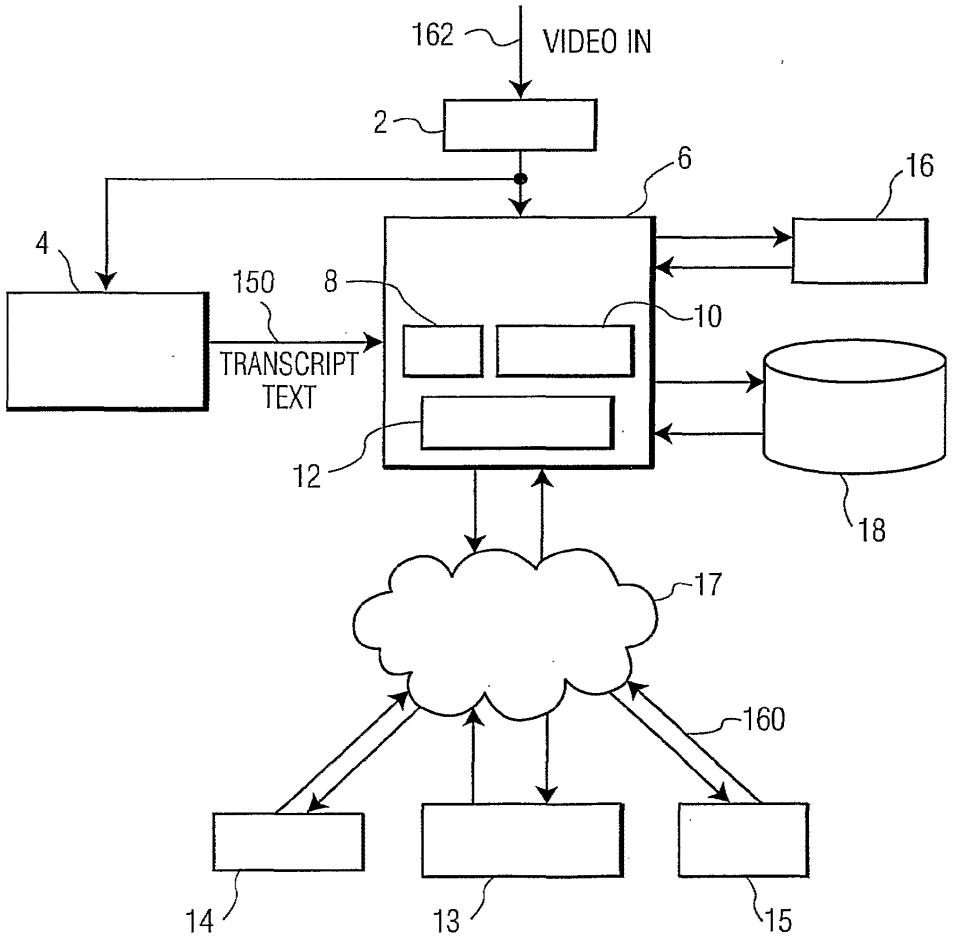

162
VIDEO IN
2
6
16
4
150
8
10
TRANSCRIPT
TEXT
12
18
17
160
14
13
15

FIG. 1

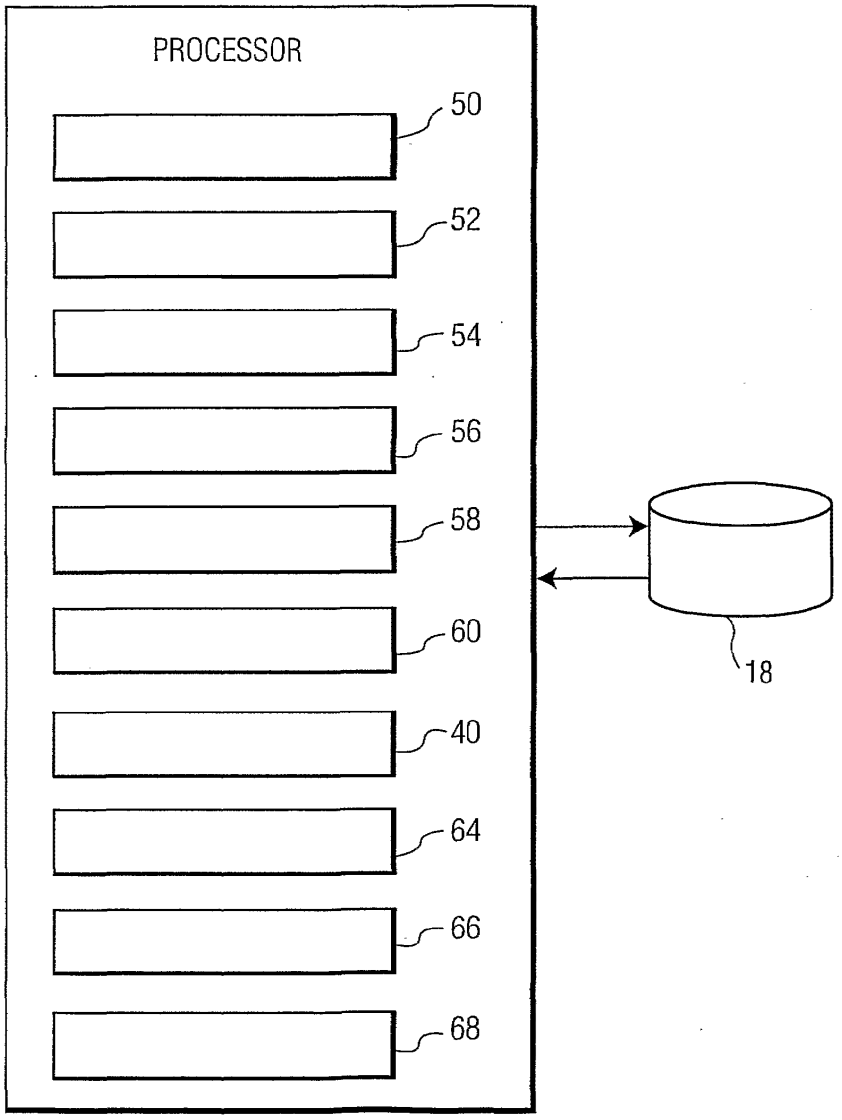


FIG. 2

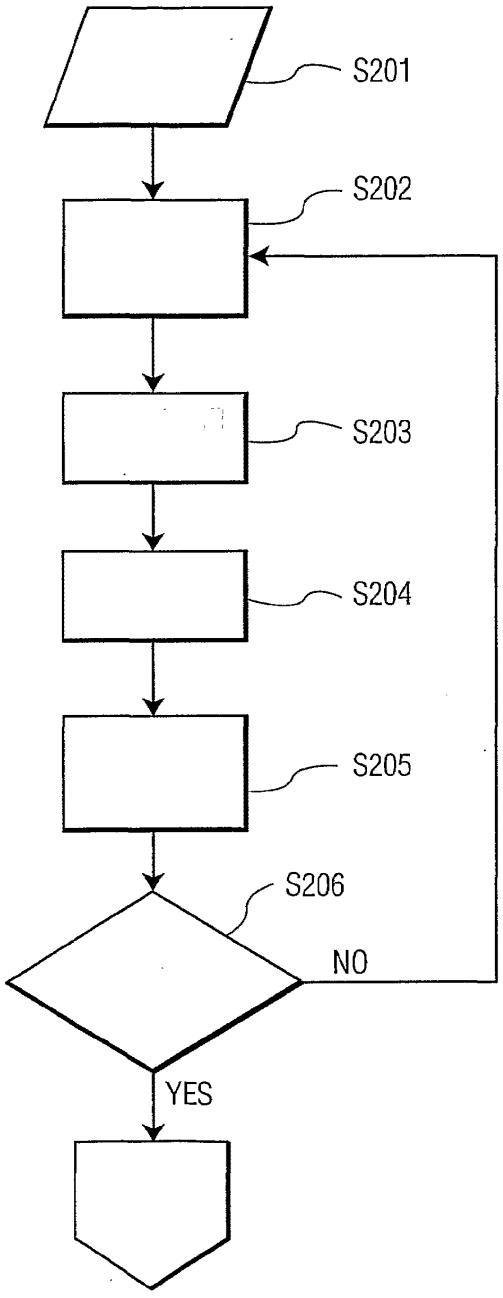


FIG. 3a

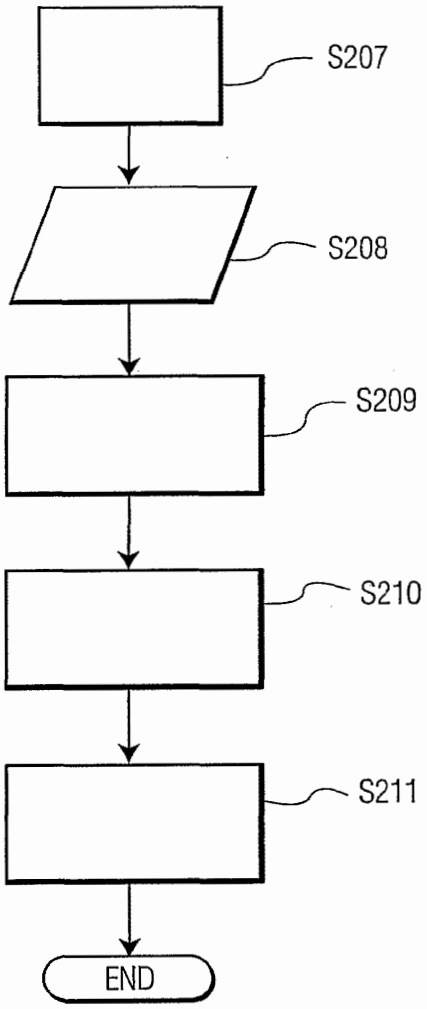


FIG. 3b

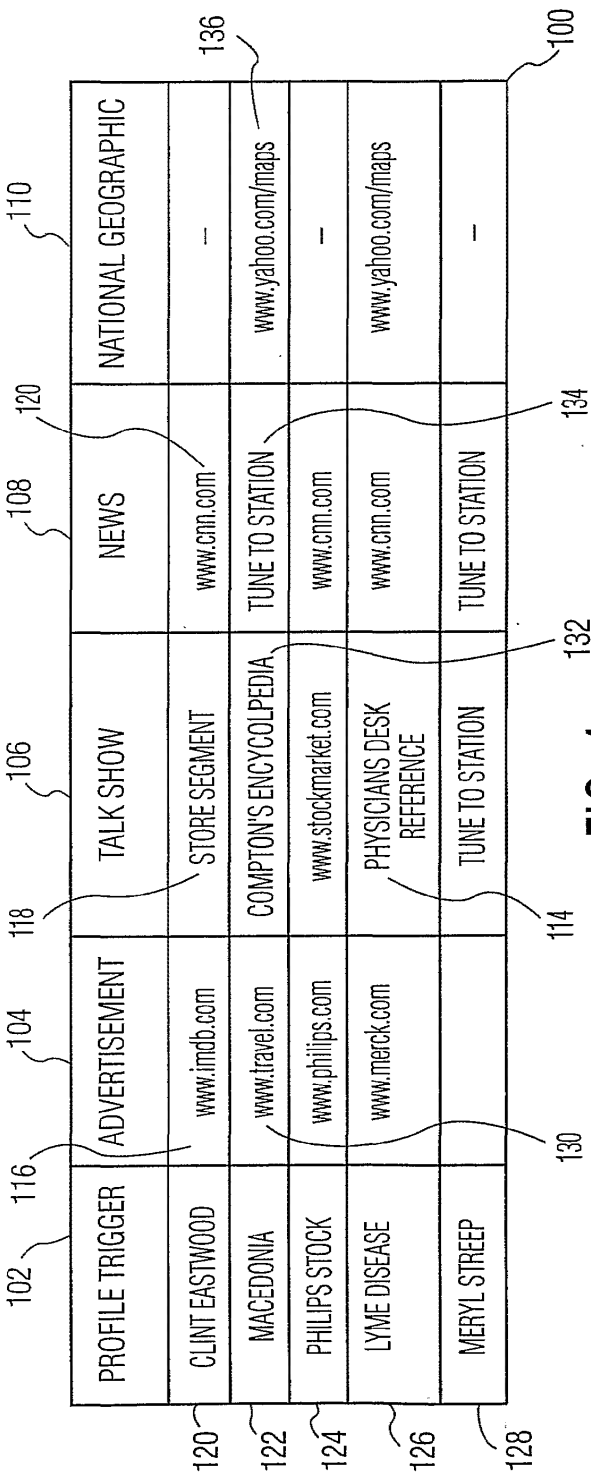

PROFILE TRIGGER
ADVERTISEMENT
TALK SHOW
NEWS
NATIONAL GEOGRAPHIC
CLINT EASTWOOD
www.imdb.com
STORE SEGMENT
www.cnn.com
—
MACEDONIA
www.travel.com
COMPTON'S ENCYCOLPEDIA
TUNE TO STATION
www.yahoo.com/maps
PHILIPS STOCK
www.philips.com
www.stockmarket.com
www.cnn.com
—
LYME DISEASE
www.merck.com
PHYSICIANS DESK REFERENCE
www.cnn.com
www.yahoo.com/maps
MERYL STREEP
TUNE TO STATION
TUNE TO STATION
—
100
102
104
106
108
110
116
118
120
120
122
124
126
128
130
132
134
136

FIG. 4

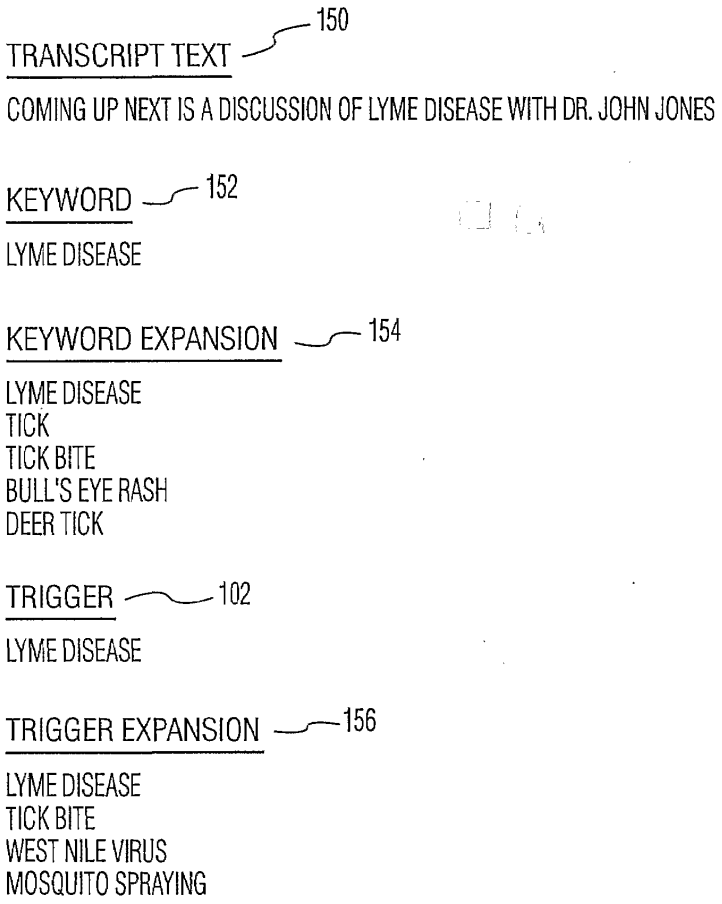

TRANSCRIPT TEXT
150
COMING UP NEXT IS A DISCUSSION OF LYME DISEASE WITH DR. JOHN JONES
KEYWORD
152
LYME DISEASE
KEYWORD EXPANSION
154
LYME DISEASE
TICK
TICK BITE
BULL'S EYE RASH
DEER TICK
TRIGGER
102
LYME DISEASE
TRIGGER EXPANSION
156
LYME DISEASE
TICK BITE
WEST NILE VIRUS
MOSQUITO SPRAYING

FIG. 4a

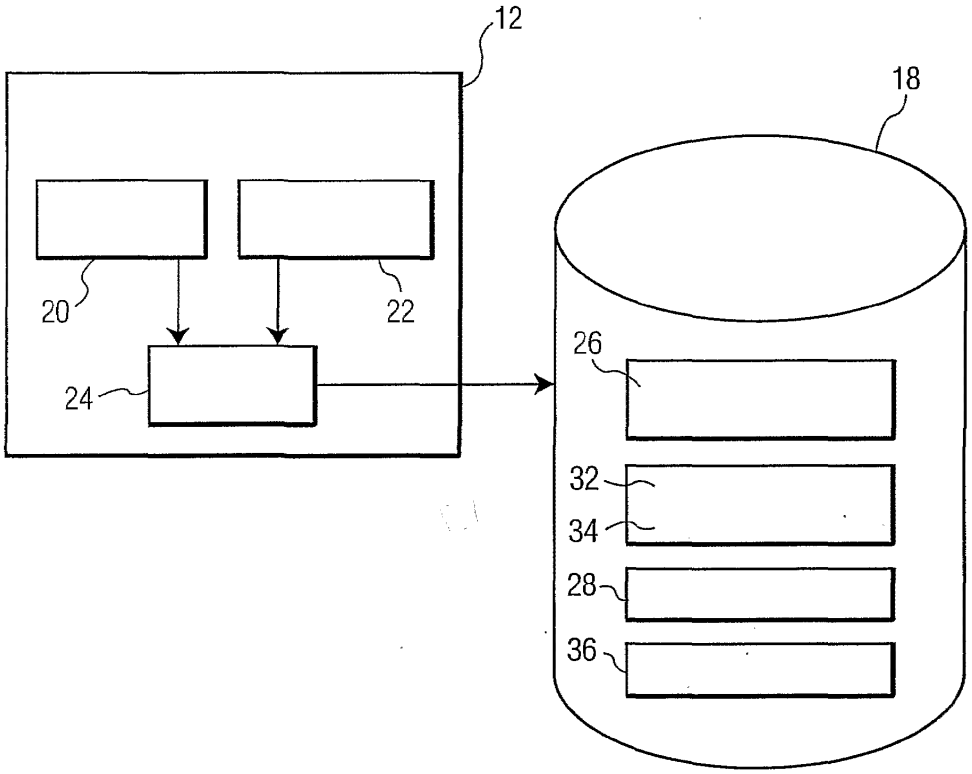


FIG. 5

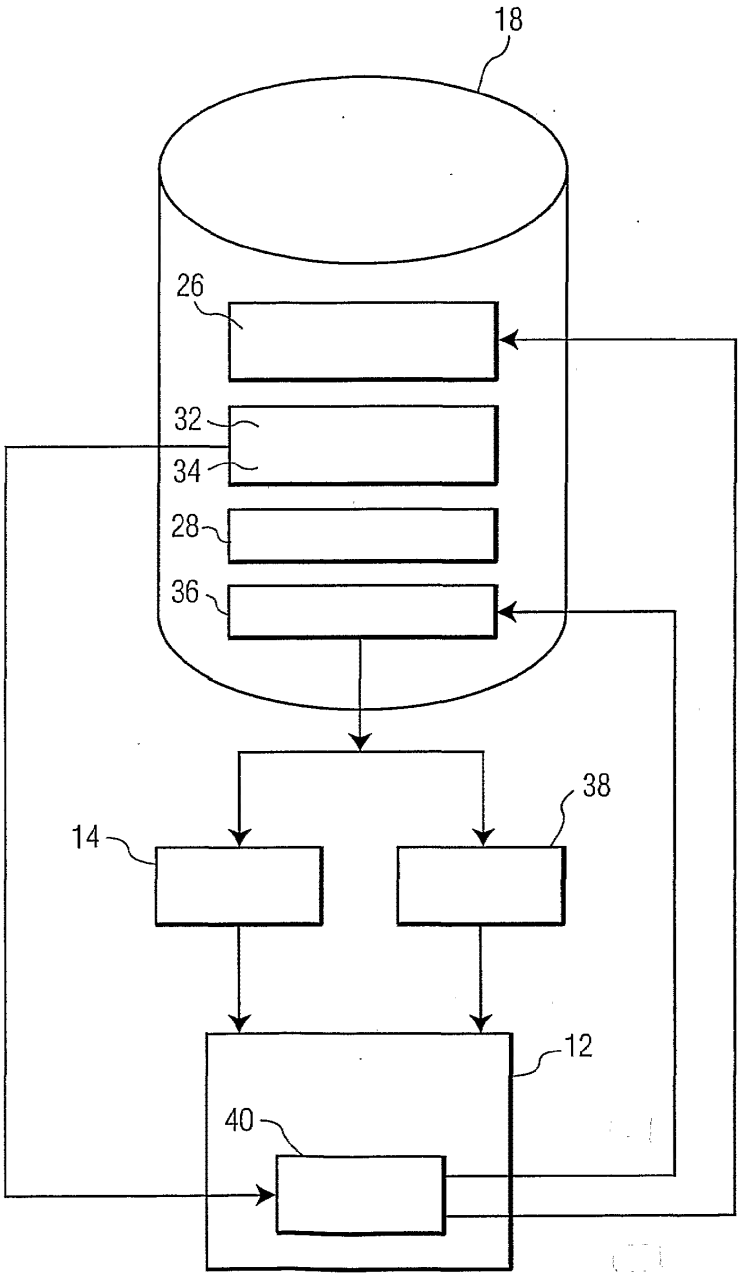


FIG. 6

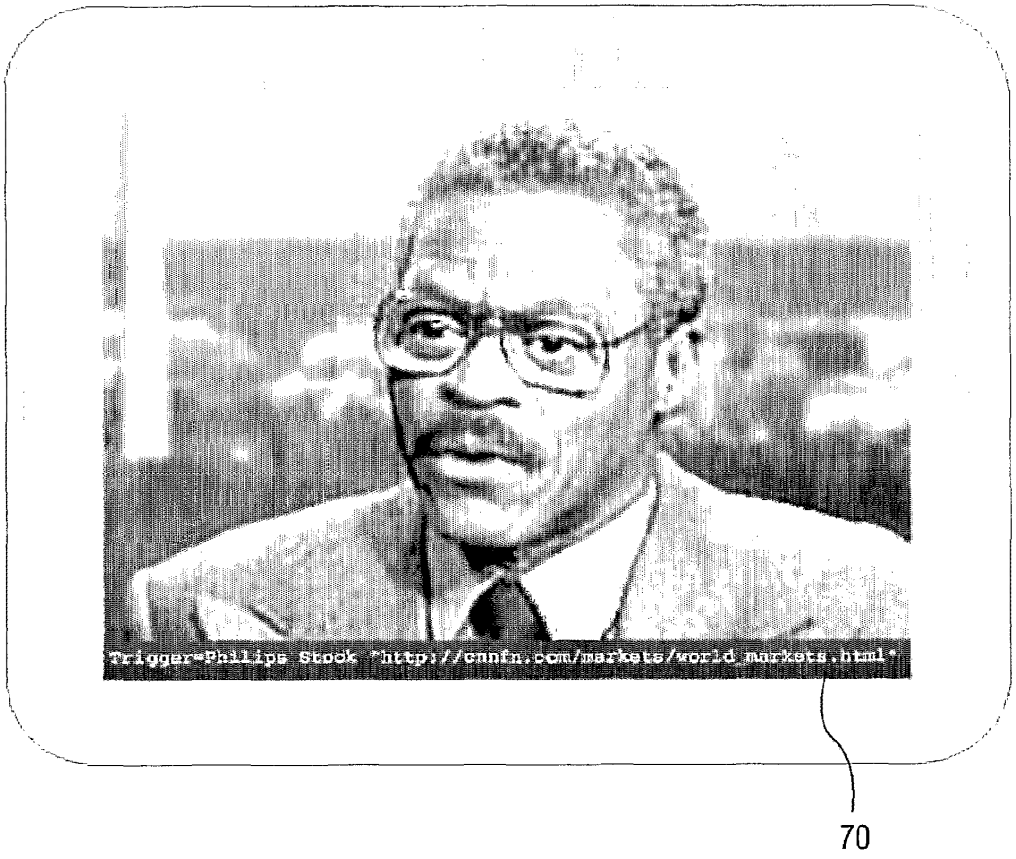

Trigger=Philips Stock "http://cnnfn.com/markets/world_markets.html"
70

FIG. 7

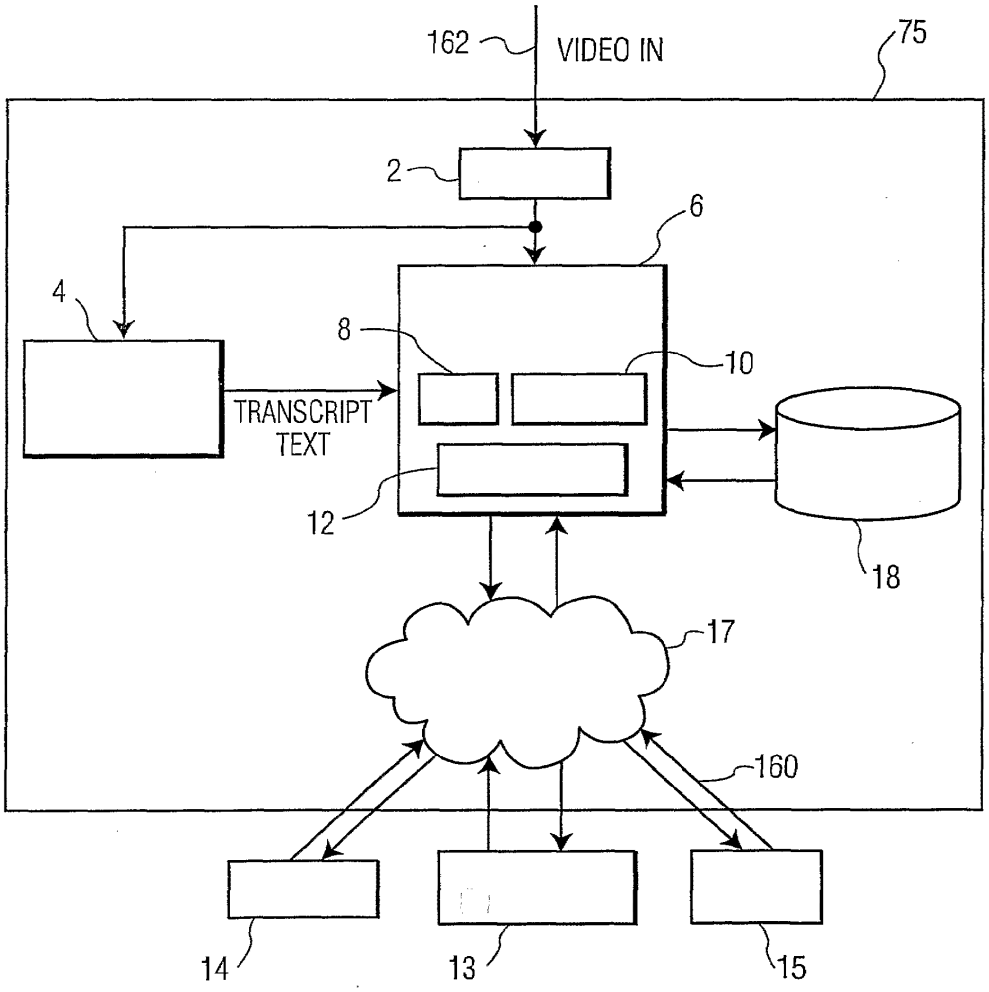


FIG. 8

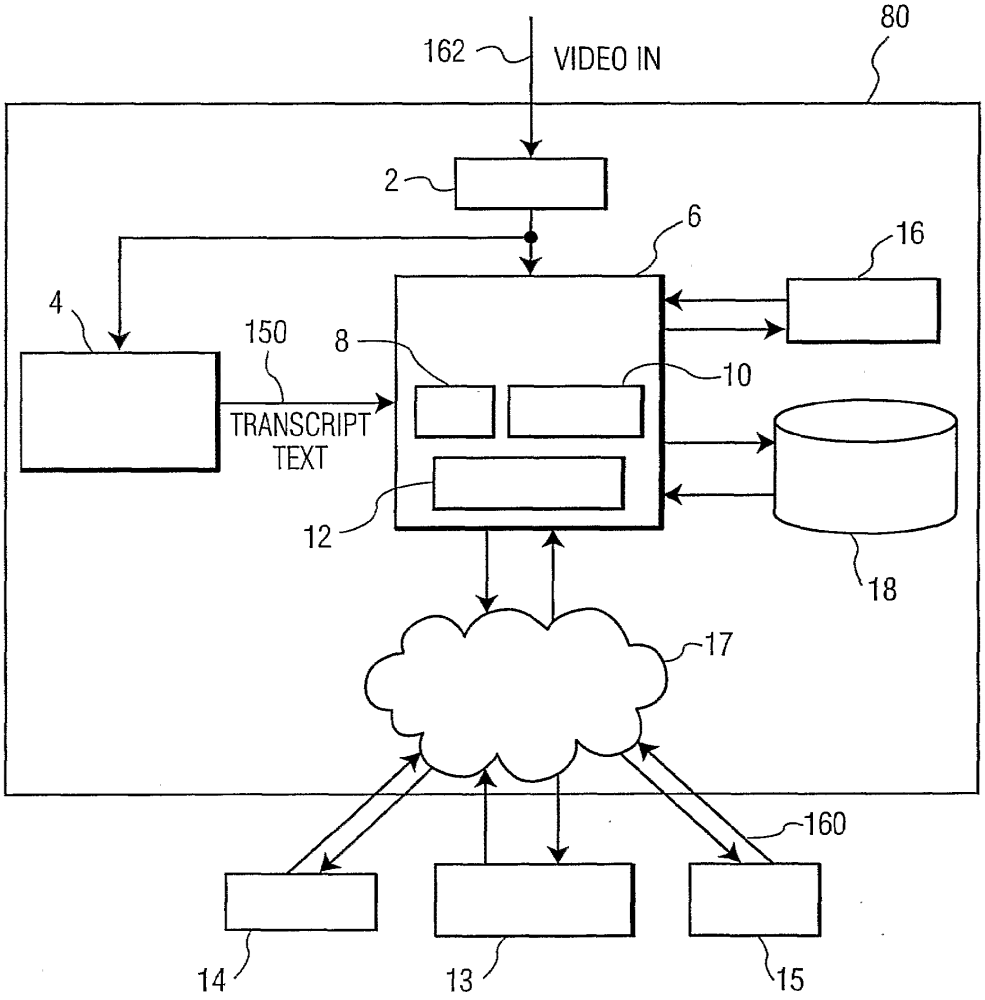

80
162
VIDEO IN
2
6
16
4
150
8
10
TRANSCRIPT
TEXT
12
18
17
160
14
13
15

FIG. 9

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **G06K 9/00**	**A1**	**(11) International Publication Number:** **WO 98/27510** **(43) International Publication Date:** 25 June 1998 (25.06.98)

(21) International Application Number: PCT/US97/23291

(22) International Filing Date: 16 December 1997 (16.12.97)

(30) Priority Data:
08/772,188 19 December 1996 (19.12.96) US

(71) Applicant: THE REGENTS OF THE UNIVERSITY OF CALIFORNIA [US/US]; Business & Patent Law, Mail Stop D412, Los Alamos, NM 87545 (US).

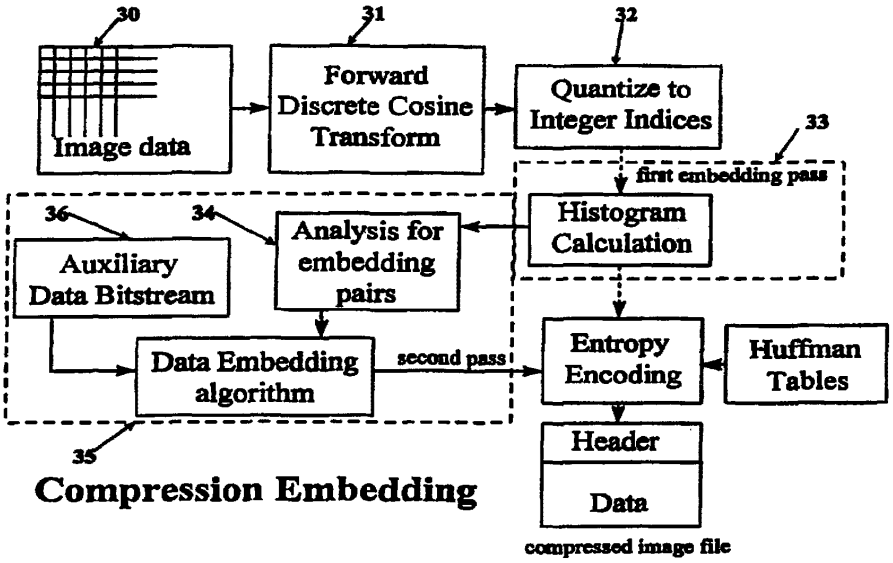
(71)(72) Applicants and Inventors: SANDFORD, Maxwell, T., II [US/US]; 160 Monte Rey Street, Los Alamos, NM 87544 (US). HANDEL, Theodore, G. [US/US]; 316 Bryce Avenue, Los Alamos, NM 87544 (US). BRADLEY, Jonathan, N. [US/US]; Apartment 512, 505 Oppenheimer Drive, Los Alamos, NM 87544 (US).

(74) Agents: WYRICK, Milton, D. et al.; Los Alamos National Laboratory, Mail Stop D412, Los Alamos, NM 87545 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, 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: COMPRESSION EMBEDDING



(57) Abstract

A method and apparatus for embedding (35) auxiliary information into the digital representation of host data created by a lossy compression technique are presented. Also presented are a method and apparatus for constructing auxiliary data (36) from the correspondence between values in a digital key–pair table with integer index values existing in a representation of host data created by a lossy compression technique.

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		

COMPRESSION EMBEDDING

FIELD OF THE INVENTION

The present invention generally relates to digital manipulation of numerical data compressed by 'lossy' compression methods. More specifically, the invention relates to a means for the embedding of external data into the intermediate numerical values determined by the lossy compression method. 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.

BACKGROUND OF THE INVENTION

This is a continuation-in-part application out of U.S. Patent Application Serial Number 08/442,592, filed May 17, 1995.

The use of data in digital form is revolutionizing communication throughout the world. Much of this digital data communication is over wire, microwaves, and fiber optic media. When it is necessary to transmit large amounts of data, innovative methods to minimize the communication time are required. Transmissions of digital television, for example, use data compression methods to accomplish this minimization. A class of these methods is termed "lossy compression." The class is termed 'lossy' because the compression methods reduce slightly the quality of the original data. Multi-media computing applications use lossy compression of image and audio data to improve performance and reduce data storage requirements.

In many situations, it may be of benefit to send particular secondary data along with the primary data. Secondary data could involve the captioning of television programs, identification information associated with photographs and audio signals, data to authenticate or validate the host information, data impressed as a digital watermark signature, or command data, i.e., Java byte codes, transmitted with images in the Internet.

Authentication using a separate electronic indicia is taught in U. S. Pat. No. 4,949,381; to: Pastor; issued Aug. 14, 1990, assigned to Pitney Bowes, Inc., Stamford, Conn. This application teaches another method, wherein no separate indicia is required to convey the hidden information. The machine readable secondary, or auxiliary data reside entirely within the content of the host data. The auxiliary data are invisible to humans, and require a digital

key to be constructed from the host information by machines. The digital key may be protected by the use of "public key" encryption systems, such as the generally known RSA encryption system.

This application employs invisibility provided by manipulating the host information in a manner similar to the disclosures in copending application serial number 08/392,642, filed February 23, 1995, for DATA EMBEDDING. Auxiliary data embedded into the host information are constructed by processing machine readable, digital host data. Human readable versions of the host data, images displayed on screen or printed from the digital forms, cannot be scanned or processed to construct the auxiliary information. Data embedding as taught in the above copending application creates and manipulates a copy of the original image. The machine readable copy of the host image is manipulated to convey the added information. The amount of host information, i.e., the number of bits it contains is unchanged by data embedding, in contrast with authentication as taught by Pastor, who creates a separate, visible bit-mapped electronic indicia.

Authentication of the host data constitutes the successful construction of all or part of the auxiliary data embedded into the host information, because any modifications changing the host data representation preclude the invention.

In one embodiment of the subject invention, the auxiliary data are encrypted before the data embedding process in order to randomize the auxiliary bit stream and minimize the effect of embedding on the host data. However, the security of data embedded as taught in the above-mentioned copending application requires no decryption, owing to the noise-key used to control the embedding process.

In still another embodiment of the subject invention, the noise-key used to embed and construct the auxiliary data is encrypted using a public key encryption system such as RSA.

The auxiliary data can be embedded using methods to modify the noise component of the data as disclosed in the above-described copending application. However, lossy compression methods modify the noise component and degrade the fidelity of the original host data. This loss in fidelity destroys any information which has been embedded into the noise component of the host data, as is taught by the abovedescribed copending application. This means that lossy compression is incompatible with prior data embedding methods. The present invention implements the principles of data embedding to achieve the embedding of an

auxiliary data bit stream in host data compressed with lossy compression methods. The invention is particularly useful for embedding information required to remove a digital watermark from host data consisting of digital television or multi-media images compressed with lossy methods.

Redundancy and uncertainty are intrinsic to lossy compression methods. Two examples of lossy compression are the Joint Photographic Experts Group (JPEG) standard, and the Wavelet Scalar Quantization (WSQ) algorithm that has been adopted by the Federal Bureau of Investigation for the electronic interchange of digital fingerprint information. A similar compression standard established by the Moving Picture Experts Group (MPEG) is used for digital television and multi--media imagery. The JPEG and MPEG algorithms are based on the Discrete Cosine Transform (DCT) representation of the host data. The WSQ method is based on a representation of the host data in terms of wavelet functions. In the methods, the host data representation exists in an intermediate stage as a sequence of blocks of integer values referred to as 'indices.' At this intermediate stage, loss of fidelity occurs because the transform coefficients that represent the original data are quantized to a finite number of integer representations. The above mentioned JPEG, WSQ, and MPEG methods apply some form of loss-less compression to the integer coefficient blocks, resulting in doubly compressed data approximating the original image.

In the normal JPEG algorithm, the indices from the quantizer compress further with a loss-less entropy coder, usually a modified Huffman compression. An alternate method taught in U. S. Pat. No. 5,187,755; to: Aragaki, issued Feb. 16, 1993; assigned to Dainippon Screen Mfg. Co., Ltd., Kyoto, Japan represents part of the coefficient blocks by means of code tables. The code tables are established before the loss-less compression step is applied. Code tables represent parts of the coefficient blocks to within the error permitted by the standard deviation in the original pixel data. The index for a code table is used in place of parts of the coefficient matrix, thereby achieving an additional improvement in the data compression. The JPEG format is represented by ISO standards DIS 10918-1 and DIS 10918-2. The code table method is incompatible with the JPEG standards, and it therefore requires a special implementation, or a revised standard. The present application does not apply to lossy compression methods using code table representations for the coefficients in a block, because the invention manipulates the indices within a coefficient block.

Redundancy occurs in all lossy compression methods because the same integer values occur many times in the compression sequence of indices. Uncertainty occurs in the integer representation because the uncertainty in the original host data is present also in its transform representation. Indeed, the above mentioned code table compression method exploits redundancy in the integer coefficients and approximates parts of coefficient blocks with members of a plurality code table. The present invention depends upon the integer index values within a code block being individually uncertain by at least one unit of value.

Derek Upham implemented a manipulation of the quantizer parity as a means for embedding information into the JPEG algorithm (JSTEG source code May 25, 1993, available electronically at: ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/jsteg). The modified quantizer output is passed to loss less compression, and then to the compressed image file. Kineo Matsui and K. Tanaka ("Video-Steganography: How to Secretly Embed a Signature in a Picture," International Multimedia Assoc. Intell. Prop. Project. Proc., 1994) also manipulate the parity of the quantizer output, in synchronization with a bit pattern that is embedded as a repeating digital signature. Modifying parity to add information to embed information into the JPEG indices changes their statistical distribution. Modifying the quantizer parity disturbs the performance of the loss less compression process, resulting in a significant increase in the size of the compressed file size.

In the invention, the quantizer output flows to the data embedding algorithm, where key-pairs are calculated from constraints applied to the statistical distribution of the indices. Data bits from the auxiliary data modify the quantizer output according to the key-pair value correspondence, as taught in the above-described copending application. The advantage of the invention is two-fold:

1) The statistical properties of the quantizer output determine pairs of indices that can be exchanged without affecting significantly the entropy of the indices. Thus, the embedding process is nearly adiabatic, and the loss less coding performs nearly as well as it does without embedding data.

2) The histogram analysis leads naturally to a schedule of indices, or key-pair table, that drives the embedding algorithm. The security of the embedded information is high, because the embedding is done according to key-pair values that must be known to retrieve the information.

For embedding with the invention, the quantizer output flows to the data embedding algorithm, where the key-pairs and data bits from the auxiliary data are used to modify the quantizer output.

The existence of redundancy and uncertainty in the intermediate compression indices permits a process for embedding additional, invisible information into the machine readable compressed representation of the host data. Because the expansion of the compressed data returns an approximation to the original information, the adherence to the existing standards for JPEG and MPEG compression is unaffected by embedding the additional information. The embedded information is invisible to humans viewing the image expanded from the lossy compression data, and to machines reading the coefficient indices for purposes of reconstructing the host data. The auxiliary information is constructed by a machine that processes the indices and has the requisite knowledge to interpret certain of their values, in particular ones matching the key-pair schedule entries, according to their position of occurrence in the host data. The machine required to process the embedded information, for either embedding or auxiliary data construction, can be a channel in series with, or parallel to, the hardware or software implementing the compression expansion algorithm.

The embedding of information by the invention does not increase the bandwidth required for the transmission of the compressed data because the auxiliary data reside in the identical coefficient values representing the original data. The positions of the integer values within their respective blocks of coefficients are changed to embed the auxiliary data, but this manipulation is nearly adiabatic, with consequent minimal affect on the final, loss-less compression of the coefficient blocks. One may convey thereby meaningful, new uncorrelated information invisibly in the machine readable redundant coefficients of the lossy compression representation without it ever being detected by unauthorized persons.

This invention is based on the above-described copending application, but expands the data embedding principle of that application to a new regime. Compression embedding as taught in the present application is different than the data embedding as taught in the copending application because compression embedding adds additional data by manipulating the intermediate numerical representation of the host created by a lossy compression method instead of manipulating the host data values directly, as is taught in the copending application.

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 data compressed with lossy algorithms.

It is yet another object of the present invention to provide apparatus and method for allowing construction of an auxiliary data bit stream from a lossy, compressed digital information stream into which the auxiliary data bit stream has been embedded according to the present 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 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 compressed by lossy compression ratio methods that use series expansion and quantization techniques comprising the steps of creating a duplicate digital compression representation of said host data in terms of intermediate integer indices representing coefficients, the digital compression representation having certain statistical properties; creating a digital representation of the auxiliary data in the form of a sequence of individual bit values; evaluating the digital compression representation to determine pairs of integer indices differing by a specified number of units and occurring with similar frequency in the digital compression representation; replacing individual integer indices in the digital compression representation with values taken from a digital key comprising a schedule of the pairs of integer indices in order to embed individual bit values corresponding to the sequence of individual bit values of the auxiliary data; and outputting the digital compression representation with the auxiliary data embedded into a file format specified for the compressed data.

In another aspect of the present invention, and in accordance with its objects and principles, a method of constructing embedded auxiliary data from a machine readable lossy digital compression representation containing integer indices comprises the steps of creating a look-up table defining a correlation between the integer indices and the elements of a key-pair table; matching the decoded integer indices from the lossy digital compression representation with entries in the look-up table, for the purpose of determining correspondence of the integer indices with elements in the key-pair; constructing the auxiliary data according to the correspondence in the look-up table between the integer indices and an element in the key-pair table; validating the content and correctness of the auxiliary data by examining header data constructed from the correspondence between the integer indices and the key-pair values; and interpreting the auxiliary bits as data unrelated to the lossy compressed data.

In yet another aspect of the present invention and in accordance with its objects and principles, apparatus for embedding auxiliary data into individual frames of host data having integer indices of certain values and frequencies of occurrence compressed by lossy compression ratio methods that use series expansion and quantization techniques comprises buffer storage means receiving the individual frames of host data for entropy decoding, modifying and momentarily storing the integer indices of the individual frames of host data,,entropy coding said modifications to the integer indices of the individual frames of host data, and outputting the entropy coded modifications to the integer indices of the individual frames of host data. Histogram analysis means receive the entropy coded modifications to the integer indices of the individual frames of host data for processing a statistical relationship between the frequency of occurrence and the value of the integer indices of the individual frames of host data, identifying embedding pair candidates in the individual frames of host data, and outputting the embedding pair candidates. Key-pair table means receive the embedding pair candidates for creating a key-pair table for each of the individual frames of host data, and outputting the embedding pair candidates as a randomized table. Compression embedding means receive the embedding key pair table, the integer indices from the individual frames of host data retained in the buffer storage, and the auxiliary data for embedding the auxiliary data and the key-pair table into the individual frames of host data and outputting an embedded stream of individual frames of host data.

In still another aspect of the present invention and in accordance with its objects and principles apparatus for constructing auxiliary data and a key-pair table embedded into individual frames of host data compressed by lossy compression ratio methods that use series expansion and quantization techniques comprises look-up table means receiving the key-pair table from the individual frames of host data for extracting the key-pair table and outputting a key-pair index corresponding to each of the integer indices from the individual frames of host data in a buffer storage. Auxiliary data construction means receive the key pair table for each of the individual frames of host data and the integer indices from the individual frames of host data stored in the buffer storage for using the key pair to construct the auxiliary data from the individual frames of host data and outputting an auxiliary data bit stream.

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 reproduction of the gray scale image example used to describe the invention.

FIGURE 2 is a plot of the histogram of the integer representation of the image in Figure 1 compressed with the JPEG method.

FIGURE 3 is a plot of the histogram of the integer representation of the image in Figure 1 compressed with the WSQ method.

FIGURE 4 is a block diagram illustrating the processes used in the embedding of data into the integer indices of a lossy-compressed data host.

FIGURE 5 is a block diagram illustrating the construction of auxiliary data from the key-pair values and the index values in the lossy compressed data host.

FIGURE 6 is a listing of computer code used for determining the pairs of integer indices suitable for embedding data.

FIGURE 7 is a listing of computer code used for eliminating duplicate host data pairs.

FIGURE 8 is a listing of computer code that performs a randomization of the pairs of indices in order to provide security against unauthorized access to the embedded information.

FIGURE 9 is a listing of computer code that performs the actual embedding of auxiliary data into the compression representation.

FIGURE 10 is a listing of computer code that constructs auxiliary data from the key-pair values and the lossy compression host data indices.

FIGURE 11 is a block diagram illustrating the embedding method of the present invention in concert with lossy compression hardware.

FIGURE 12 is a block diagram illustrating the construction of auxiliary data in hardware according to the present invention.

DETAILED DESCRIPTION

The present invention allows data to be embedded into information compressed with a lossy method without naturally discernible alteration of the content of the compressed information or the meaning of the embedded data constructed from the compressed information. This is made possible because of the technique of the present invention, in which similar integer indices in a lossy compression representation are re-ordered according to the desired embedded or implanted information. The lossy compression examples are digital images compressed using JPEG and WSQ methods. The resulting images contain embedded information without that information being readily discernible to an unauthorized observer .

The JPEG method is given in an article by Gregory K. Wallace, "The JPEG Still Picture Compression Standard," **Communications of the ACM**, April 1991 (vol. 34 no. 4), pp. 30-44. The JPEG algorithm is used primarily for compressing digital images. A PostScript file containing a revised version of the article is available for electronic reference at: ftp.uu.net, graphics/jpeg/wallace.ps.Z. A somewhat less technical, more leisurely introduction to JPEG can be found in **The Data Compression Book** by Mark Nelson, published by M&T Books (Redwood City, CA), 1991, ISBN 1-55851-216-0. A detailed textbook about JPEG is **JPEG Still Image Data Compression Standard** by William B. Pennebaker and Joan L. Mitchell, published by Van Nostrand Reinhold, 1993, ISBN 0-442-01272-1.

The Independent JPEG-Group's C-language source code is available electronically from: ftp.uu.net (Internet address 137.39.1.9 or 192.48.96.9). The most recent released version can always be found there in directory graphics/jpeg.

The WSQ method as applied to compressing digital fingerprint images was given by J. N. Bradley and C. M. Brislawn, "The wavelet/scalar quantization standard for digital fingerprint images," **Proc. of the 1994 IEEE Intern. Symp. on Circuits and Systems,** vol.

3, pp. 205-208, 1994, and by J. N. Bradley, C. M. Brislawn, and T. E. Hopper, "The FBI wavelet/scalar quantization standard for gray-scale fingerprint image compression," **Proc. SPIE,** vol. 1961, pp. 293-304, April, 1993. Documentation for WSQ compression is available through Jonathan N. Bradley, Los Alamos National Laboratory, P. O. Box 1663, MS-B265, Los Alamos, NM 87545, and electronically from the Internet FTP site "ftp.c3.lanl.gov" in directory /pub/WSQ.

The JPEG method processes the host image in pixel blocks specified to the algorithm at the time the indices are calculated. The WSQ method compresses the host image by passing it through a series of multirate filters. In both the JPEG and WSQ algorithms, the image host data exist in an intermediate stage as a sequence of integer (16-bit signed) indices. The indices represent an image originally presented in a standard digital format. The characteristic of lossy compression that makes possible the invention is redundancy and uncertainty. Each integer index occurs typically many times in the compressed representation, and each index is uncertain in value due to uncertainty in the host data. The present invention creates a histogram of the integer indices in the compressed representation. This histogram shows the probability density of the integer values in the representation. The histogram plots the number of times a particular value occurs versus the value. For JPEG compression, values in the range ±1024 are sufficient, and for WSQ compression values in the range ±4096 are considered. A particular histogram of index values will depend on the image content, but both compression methods concentrate many values in a pattern symmetrical about 0.

Figure 1 is a reproduction of the gray scale image example. The invention works equally well with color images. The gray scale image example in Figure 1 does not represent a limit to the application of the invention. The gray scale example image is reproduced in Figure 1 at reduced scale and quality to facilitate printing. The reproduction in Figure 1 demonstrates only the nature of the image example, and does not convey a representation of the image quality appropriate to the invention. Images expanded from compression representations with data embedded are visually identical to those expanded from unmodified compression data.

Histograms of the indices for the image example in Figure 1 are shown in Figures 2 and 3, for JPEG and WSQ compression, respectively. Figure 2 shows the histogram for the JPEG compression representation, for the image sample shown in Figure 1, and compression ratio

about 12:1. The file size for the JPEG version of Figure 1 is 42953 bytes. Analysis of this image according to the invention identifies 50 pairs of values in the histogram, totaling 3573 bytes of embedding space.

Figure 3 shows the histogram for the WSQ coefficient representation of the image sample shown in Figure 1, and compression ratio about 20:1. Analysis of these coefficients according to the invention identifies 37 pairs of values in the histogram, totaling 471 bytes of embedding space. The WSQ histogram contains fewer coefficients than produced by the JPEG method owing to the larger compression ratio, but the invention nevertheless permits embedding information into the compressed representation.

The actual embedding of the auxiliary data into the compressed representation of integer indices in the JPEG algorithm is a two-part process, the steps of which are shown in Figure 4. The steps of the invention are shown in the dashed-outline portion of Figure 4.

The JPEG algorithm divides the original, host image 30 into blocks of 8 x 8 pixels. The pixel values within a block are converted to coefficients in a discrete cosine transform 31, and the coefficient values converted to indices by a quantizer 32. In the first invention step 33, the quantizer indices, representing the transform coefficients, are examined to identify pairs of the integer indices having values that occur with approximately the same statistical frequency, and that differ in value by only one unit. A key-pair table 34 is constructed from the histogram of the quantizer indices. The order of the integer indices key-pair values is randomized to generate a unique key sequence that cannot be duplicated by an unauthorized person.

In the second invention step 35, the pairs of indices identified from the histogram analysis are used in a second pass through the image to re-order the quantizer indices in accordance with the correspondence between the key-pair values and the bit values in the sequence of auxiliary data bits 36. The key-pair sequence 35 is saved separately, as a small binary data file.

The method for constructing auxiliary data from a key-pair schedule and the indices in a lossy compressed data host is shown in Figure 5. The key-pair sequence 41 of pairs of index values is recovered from the compressed data file 40 as taught in the above-described copending application, or it is supplied as information separate from the compressed data. The key-pair table 41 specifies the pair-values of indices differing by one unit in value, and

the order in which indices are used to construct the auxiliary data. The indices of the pairs in the key-pair schedule are used to construct a look-up table 42. For every quantizer index value that is possible, the value of a corresponding key-pair index is given. Index values having no correspondence with a key-pair, i.e., quantizer index values that are not used for embedding are assigned the index value -1.

The lossy compressed data residing in the host file 40 are processed with the appropriate entropy decoder, usually the Huffman table algorithm 43, to recover the quantizer index values. The quantizer index value is used as an entry in the look-up table to determine the key-pair corresponding to the index value. If the look-up table entry is -1, there is no corresponding key-pair and the next value from the entropy decoder is examined. If the look-up table indicates a correspondence, the index value is compared with the corresponding key-pair values (44). The key-pair value matching indicates the auxiliary bit value to be added to the bit stream 45 being constructed. If the index value is identical to the first element of the key-pair, the auxiliary bit value is zero, and if the index value is identical to the second key-pair element, the auxiliary bit value is one.

As the quantizer index values flow from the Huffman decoder 43 and the look-up table is applied 44, the auxiliary data bit stream 45 is constructed. The key-pair data are used first to construct header information. The header information specifies the length and the file name of the auxiliary data, and serves to validate the key. If the compressed host file contains no embedded information, or if the incorrect key sequence is used, the header information cannot be interpreted correctly. However, successful interpretation of the header data guides the construction of the auxiliary data.

As shown in Figure 5, the invention constructs the auxiliary data 45 without requiring an expansion of the lossy compressed data to a host image, i.e., there is no particular correspondence of the values in the look-up table 42 with the pixel values in the decompressed image. If decompression to an image is required, the auxiliary data construction method can proceed as an optional, parallel process. However, if construction of the auxiliary data 45 alone is required, the invention proceeds as shown in Figure 5.

The principle of data embedding according to the present invention involves the rearrangement of certain intermediate, integer values in a lossy compression representation in order to encode the values of the auxiliary data which is to be added. For the purposes of this

description of the invention, consider the compression representation to consist of a sequence of integer values or indices. Further assume that any intermediate index value is uncertain by ±1 unit in value. The frequency of occurrence or histogram value of a certain index i is f(i).

Two values i and j in the table of indices are candidates as embedding pairs if:

$$|i - j| = 1. \qquad 10$$

Index values meeting the criterion of Equation 10, and occurring also in the representation with $f(i)-f(j) < \delta$, where f(i) and f(j) are the probability of occurrence of adjacent intermediate index values, and δ is the tolerance imposed for statistical equality, are candidates for embedding use. The values i and j meeting this constraint constitute a pair of index values p_k. There are $k=0,1,2,...N_p$ such pairs in the compression representation, giving a total number M of embedding bits:

$$M = \sum_i f(i) + \sum_j f(j). \qquad 20$$

The summations of i and j run over a limited range of the intermediate indices. In the example given here, for JPEG compression, the summation limits are specified at ±1024.

It is now helpful to refer to Figure 6, wherein a partial listing of computer code in the C-language is printed. On the first pass through the lossy compression algorithm, the histogram table is filled with the number of occurrences of each index value, in the range from **MINVAL** to zero, and from zero to **MINVAL** (positive). For the JPEG algorithm, the range is (-1024,+1024). In the histogram analysis, the indices falling within the range ± **HISTLIMIT** are excluded from analysis as embedding pair candidates, because the low frequency coefficients affect markedly the appearance of the reconstructed image. The routine **jhistgm()** in Figure 6 accepts three calling arguments (line 57 in Figure 6, page 2). The first argument is a pointer to the histogram table that was valued during the first pass through the lossy compression algorithm. The second two arguments are pointers to the table of key-pairs, and the number of pairs. The latter two arguments are filled in value by the routine.

The histogram constraint applied in the loop starting at line 66 determines the candidate pairs. A detailed discussion of this loop code is given by Sandford and Handel in "The Data Embedding Method," Los Alamos National Laboratory report LA-95-2246UR, in **Integration Issues in Large Commercial Media Delivery Systems**, Proc. SPIE, **2615**, 226, ed. A. G. Tescher and V. M. Bove, Jr. (Philadelphia, PA 23-26 Oct. , 1995). Briefly, the pair values must differ by no more than one unit in value, and they must occur with a difference in frequency less than the average frequency for the two index values. Figures 2 and 3 show the histogram data for sample JPEG and WSQ compression representations. The code in line 76 in Figure 6, page 2, compares the absolute difference of the frequency of occurrence f(i) and f(j) with the average value of the two occurrence frequencies. Pairs differing by less than the average value are accepted in this example.

This simple selection scheme prevents an artificially large modification to the indices in the lossy compression representation. For example, if f(i)=1000 and f(j)=300, the absolute difference is 700 and the average is 650. This pair would be *rejected* as an embedding candidate. However, if f(i)=1000 and f(j)=750, the absolute difference and the average are 250 and 875, respectively, and this pair would be *accepted.* This, or a similar scheme for selecting pairs for approximate equality of their component's frequency of occurrence minimizes the effect of embedding on the performance of the entropy coding algorithm. Additionally, it minimizes the perceptible differences in the image expanded from the compressed representation containing embedded data.

The pairs selected from the histogram are stored in the data structure array element **pair[j]** in lines 77,78,and 79 (Figure 6, page 2). In the example in Figure 6, the data structure permits **MAXPAIRS** pairs to be selected. The structure element **pair[j].count** contains the total number of occurrences of the (i,j) values in the histogram table. Line 90 (Figure 6, page 3) uses the routine **duplicate()** to remove duplications from the pair table. The return value is the total number of pairs, **no_pairs**. The loop starting at line 91 calculates **lsum**, the total number of bits that can be embedded into the compression indices. The variable M, in Equation 20 defines the calculation performed in the loop starting at line 91.

The total amount of embedding space is tested against the size of the auxiliary file plus the size of the header in line 105 (see D. Upham 1993 for details). If the total embedding bit

count is less than the amount needed to store the auxiliary file and its header, an error message is printed and the number of pairs value is set to zero.

If embedding space sufficient to hold the auxiliary data exists, then the number of pairs found by the analysis is *reduced* to the minimum number required to hold the auxiliary information. For Upham's (1993) method of quantizer parity modification, the index modifications cease after the auxiliary file is embedded. Thus, there is a strong potential for a transition in image quality at the point in the image where the pixel blocks cease to be modified. In the invention, the pair values chosen for embedding exist throughout the image, in nearly all of the coefficient blocks. The loop to reduce the number of embedding pairs begins at line 111 in Figure 6, page 3.

After trimming the number of pairs, a routine is called to scramble the pair values. This routine performs two functions. It randomizes the sequence of pair values and it randomizes the correspondence between the auxiliary bit values and the elements within a key-pair. In the implementation shown in Figure 6, the pair order is not important because the auxiliary data bits are embedded sequentially into whichever is the next index value matching *any* pair in the key. To implement the order of the pairs in the key into the embedding process, the auxiliary data must be partitioned into blocks of bits, with each block corresponding to a particular key-pair.

However, the order of the elements within a key-pair is randomized, and this affects the embedding process. For example, if the first key-pair has elemental values (4,5), then the occurrence of an index value of 4 is taken to signify a zero-bit in the auxiliary file, and the occurrence of a 5, a one-bit. For another pair, say (8,9), the randomization might reverse the interpretation. Thus the pair would contain the elemental values (9,8) and 9 would correspond to a zero-bit in the auxiliary data. It is insufficient to know only the key-pair values. One must know also the *order* in which the values are assigned to correspond to auxiliary data bits, and if the auxiliary data is embedded in blocks of bits, the sequence in which the key-pairs correspond to the blocks.

The embedding process ignores completely the contribution the index values make to the compression representation. In JPEG compression, the values represent the coefficients in a discrete cosine transform performed over pixels in a square block of the image data. Usually, 8x8 pixel blocks are used, but the details of the transform and the tiling of the image data are

irrelevant for the invention. In WSQ compression, the indices are determined by quantizing the discrete wavelet transform coefficients which are calculated by repeated applications of a multirate filter bank. Again, details of the wavelet calculations and the sampling size are ignored in the selection and use of the embedding pairs.

Depending on the details of the selection algorithm, the key-pairs found can include generally redundant values. The same index value i, is found perhaps in several different pair combinations. Because multiple pairs cannot contain the same index entry, due to each pair combination of index values having to be unique, it is necessary to eliminate some pairs.

Referring now to Figure 7, the code fragment listed therein illustrates the manner in which duplicate pairs are eliminated by a separate routine. First, the histogram of the image is used to calculate the total number of occurrences of key-pair structure elements, with the code in Figure 6. The key-pair selection algorithm given in Figure 6 results in pairs being selected in ascending index order. Before rejecting some pairs, the pairs are sorted in line 23 of Figure 7, page 1 by order of decreasing frequency of occurrence value, **pair[j].count.** Sorting the pairs by occurrence frequency before rejecting duplicate pairs minimizes the number of pairs needed to embed a particular auxiliary data bit stream. The nested loops beginning at line 24 of Figure 7, page 1 reject duplicate pair values containing the fewest occurrence frequencies. The routine revises the pair structure elements in the loop starting at line 47 (Figure 7, page 2) and returns the new ***no_pairs** value.

The security of the embedded data is increased significantly if the pair values are arranged into random order. Randomizing the order of the pair values is part of this invention and follows the code listing in Figure 8. Randomizing is accomplished by rearranging the pair values according to a randomly ordered data structure. Two routines serve to randomize the key-pair values. The routine **scramble()** starts at line 20 in Figure 8, page 1, and the routine **jumble()** starts at line 74 in Figure 8, page 2. An ordered sequence of integers in the array named **index[]** is randomized by the **jumble()** routine. The random indices are used to re-order the key-pairs in a loop starting at line 34. The re-ordered data structure replaces the original key-pair data in line 39. In another loop starting at line 46 in Figure 8, page 2, the correspondence of the pair elements with the auxiliary bit values is randomized.

In the **jumble()** routine, the structure named **pts** contains elements **pts[k].i**, k=0,1,2,..., **no_pairs**; and **pts[k].gamma**, $\gamma_1,...,\gamma_k,...\gamma_{no\_pairs}$, where the γ_k values are uniformly random on

(0,1). The structure values are assigned in the loop starting at line 82 in Figure 8, page 2. The standard library routine **qsort()** is used to sort the data structure **pts[]**. Putting the random element values into ascending order randomizes the index element of the structure. The random index values are used with the pair structure elements calculated and sorted as indicated above, to re-order the table to give random pair ordering.

The actual embedding of auxiliary data into a compression representation consists of rearranging the order of occurrence of the redundant indices. A fast embedding implementation results by using a table look-up in place of the exhaustive search that was given previously in the above mentioned work by Sandford and Handel (1995). Figure 9 contains the code for the **Embed_Data_Block()** routine. The routine includes several static variables (Figure 9, lines 38-40, page 1; lines 44-49, page 2). The variable **ptable[]** is an array that contains the index of the pair that corresponds to any value of the quantizer output, also an index.

The arguments to the routine entry at line 55 in Figure 8, page 2, are a pointer to a buffer containing quantizer index values and the number of values that are to be processed. To find the embedding pair structure that corresponds to any quantizer output value, the value is offset by the minimum amount and used as an index into the **ptable[]** array. The value taken from **ptable[]** is the index to the correct pair of embedding values. Values in the **ptable[]** set to -1 indicate there is no correspondence with embedding key-pair values. Thus, quantizer values giving negative **ptable[]** values are ignored, and those giving **ptable[]** values greater than, or equal to zero, are used to embed one bit of auxiliary data. A static variable named **ptable_filled** is used to indicate that the **ptable[]** array must be initialized from the key. The test at line 61 in Figure 9, page 2 permits reading the binary key-pair file and setting the **ptable[]** values.

Data embedding is accomplished by the loop starting at line 97 in Figure 9, page 3. For each quantizer index value in the input buffer, the data embedding algorithm (Sandford and Handel 1995) is applied. The routine **bitgetbit()** (see Upham's 1993 JSTEG code for details) supplies the value of the next bit in the header or the auxiliary data file. Upon exhaustion of the auxiliary bits, the return value (line 103) is -1, and the embedding is completed. The commented line 107 is activated if it is desired to generate a 'marked' output image that shows the locations in the host data that are used by the key-pair values.

The key-pairs selected for embedding contain the index values to be used in the rearrangement. It is important to realize that the numerical values used for embedding data are the index values already occurring in the compression representation. The maximum pair table size permitted depends upon the compression representation. For JPEG compression, Figure 2 shows the index values concentrate near the origin and 50 to 100 pair values are adequate. For WSQ compression of digital fingerprints, the index values spread over a larger spectrum and more pairs are required.

A consequence of the histogram constraints used to determine the key-pairs is that the current invention alters the entropy in the DCT or WSQ coefficients only slightly. Thus, the efficiency of loss less compression is largely unaffected by embedding auxiliary data into the indices values.

In the embedding process of the present invention, the coefficients calculated by the compression algorithm are manipulated in the order they appear from the compression scheme used to generate the representation, JPEG and WSQ for the examples herein. The embedding process flows concurrently through the sequence of auxiliary data bits and the compression indices. Upon identifying a compression index matching one of the pair table values, the next bit in the sequence of auxiliary data is examined to determine if the index is set to the **pair[k].i** value (embedding a 0), or set to the **pair[k].j** value (embedding a 1). The key-pair table is processed sequentially, in the order found after it was randomized by the code in Figure 8.

The standard "Lena" test image is used to compare the results of the invention with JPEG baseline compression and quantizer parity steganography as implemented by Upham (1993). A 1288-byte test file (jembed.obj) is used as the auxiliary data, and the identical header procedure is implemented for the comparison.

Table 1 gives the file sizes for the original Lena image (lena_rgb.tga), for JPEG baseline compression of the original 24-bit Truecolor image (lena.jpg), for quantizer parity steganography with the JSTEG method (lenau.jpg), and for the invention (lenax.jpg). The Truecolor image compresses to the baseline JPEG standard with ratio 18.88:1 from the original size. With 1288 bytes embedded (3 % of the compressed size), quantizer parity steganography increases the compressed file size by 801 bytes (1.9 %), giving 18.52:1 compression ratio. The invention increases the file size 16 bytes (0.038 %) giving 18.87:1

compression ratio. Quantizer parity steganography increases the compressed file size by 62 % of the auxiliary file size. The present invention increases the compressed file size by 1.2 % of the auxiliary file size. Thus, the Lena test image demonstrates that the present invention affects minimally the compression efficiency of the JPEG algorithm.

Table 1. Test Images for 1288 bytes

file name	file size (bytes)
lena_rgb.tga	788,019
lena.jpg	41,747
lenau.jpg	42,548
lenax.jpg	41,763

The construction of auxiliary data from a lossy compressed host containing embedded data is achieved by processing the entropy decoded quantizer coefficients with a look-up table. Figure 10 gives the listing of code to construct auxiliary data from the quantizer indices. The routine named **ExtractDataBlock()** processes a buffer of quantizer indices and constructs the auxiliary bit stream associated with the key-pair values. The routine uses static variables (see lines 19 to 23 in Figure 10, page 1) for the look-up table **ptable[]**, a flag named **ptable_filled** to signify that the **ptable[]** array requires filling from the key-pair schedule, and a variable named **embed_count** to count of the number of auxiliary bits constructed. The subroutine begins at line 43 in Figure 10, page 2, and it accepts two arguments. The first argument is a pointer to the buffer containing integer values of the quantizer indices, and the second argument specifies the number of values in the buffer.

If the **ptable[]** look-up array requires filling, the key-pair schedule is read from a binary data file at line 57 in Figure 10, page 2, and the look-up table is filled with indices indicating the correspondence between the key-pair values and the quantizer indices. The loop starting at line 81 in Figure 10, page 2 processes the quantizer indices in the input buffer. If a correspondence between a quantizer index value and an entry in the key-pair table exists, the quantizer index is tested against the key-pair value elements to determine if the auxiliary bit is zero or one. The routine **bitsetbit()** is used to add one bit of the appropriate type to the auxiliary bit stream being constructed (see Upham 1993 for details). The **bitsetbit()** routine

returns -1 when the auxiliary data file is completely constructed. The return value is tested at line 88 in Figure 10, page 3.

Owing to the uncertainty introduced by randomizing the order of the key-pair table, the auxiliary data are secure against unauthorized construction from the compression representation. Indeed, detecting the presence of embedded data is difficult, if not impossible, because the only metric known to us for such detection is a statistical analysis of the compression representation indices. Because the invention affects the statistical properties only slightly, it leaves no characteristic signature revealing the presence of embedded information.

As previously described, the ordered pairs of index values selected for embedding constitute the "key" for construction of the auxiliary data from the compressed image. The listings illustrated in Figures 6 through 10 demonstrate how embedding analysis exploits redundancy and the statistical uncertainty in the compression representation to construct a look-up table of key-pairs of index values. The key-pairs are required for constructing the auxiliary data, but they cannot be generated by analyzing the compressed image representation after the embedding process is completed. The invention retains the one-time-pad encryption properties inherent in data embedding as disclosed in the above-described copending application, and incorporates the same high security to the embedded bit stream.

As for data embedding as disclosed in the copending application, another way of protecting the pair table key is to encrypt it using public-key or another encryption process. The present invention permits an encrypted key to be placed into the compressed file, preventing extraction by unauthorized persons.

Embedding auxiliary data into the compression representation slightly changes the statistical frequency of occurrence of the index values. If the auxiliary bit sequence is pseudo-random, the frequencies of occurrence for the index pairs i and j are nearly equal after embedding. Equalizing the histogram reduces entropy somewhat, and the entropy coding portion of the compression algorithm is found often to operate with slightly *greater* efficiency, increasing the effectiveness of the lossy compression method. Thus, even if no auxiliary information is to be embedded, equalizing the statistical properties of the histogram pairs improves the compression ratio for lossy methods. Embedding pseudo-random, or white noise to improve compression is part of this invention.

The present invention can be implemented into existing lossy compression machines, as shown in Figure 11. In the upper left of Figure 11, a standard, composite video signal 11 is input to encoder chipset 12 which encodes composite video signal 11. The binary output 13 of encoder chipset 12 consists of sequences of Inter-frames (I-frames), motion vector information, and Backward- and Forward-predicted frames (B,P-frames) and, when auxiliary information is to be embedded, passes via the dashed path to buffer 15 of embedding chipset 14.

Embedding chipset 14 consists of the functions within the dashed box in Figure 11. Embedding chipset 14 provides the functions which implement the present invention. As illustrated, buffer 15 entropy decodes, modifies and momentarily stores the integer indices of the individual frames of host data in preparation for the subsequent embedding procedure. The modification of the integer indices is conducted as described hereinabove in this specification, after which buffer 15 entropy codes the modifications to the integer indices. These modified integer indices are then output to histogram analysis 16, where the statistical relationship between the frequency of occurrence and value of the modified integer indices is processed in order to identify appropriate embedding pair candidates. These embedding pair candidates are output to key-pair table 17. Key-pair table 17 processes the embedding pair candidates to generate a key-pair table for a frame of binary output 13 which is stored in buffer 15.

Compression embedding engine 18 receives each frame of buffered binary output 15 as well as the output of key-pair table 17 and auxiliary bit stream 19. Compression embedding engine 18 embeds auxiliary bit stream 19 into the I-frame indices of buffered binary output 15, and the modified I-frame indices are compressed along with the key-pairs to produce embedded MPEG-2 bit stream 20

The processing time for embedding auxiliary data with the present invention is less than the time required to encode an I-frame and its associated motion-predicted frames (B- and P-frames), thereby maintaining the output rate of the MPEG-2 data stream. The key-pair table for the I-frame is inserted into the motion prediction portion of the MPEG-2 data, or it is added as a fictitious frame. Thus, the key-table data appear as an MPEG-2 coding error that is ignored by MPEG-2 decoding machines.

It should be understood that, although Figure 11 illustrates chipset 14 for implementing the present invention, the functions of chipset 14 could also be implemented in circuit board circuitry. Such implementations could be useful for limited applications of the present invention.

In Figure 12, apparatus for constructing auxiliary data from an embedded MPEG-2 bit stream is illustrated. The embedded MPEG-2 signal 21 is processed in parallel with a conventional MPEG-2 decoder 22 that generates composite NTSC standard video 23 for viewing. The present invention, in the parallel leg within the dashed box in Figure 12, obtains the key-pair table from the MPEG-2 entropy-decoded bit stream data and generates a look-up table 24 from the key-pair table to permit processing the embedded I-frame integer indices by auxiliary data construction 25. Auxiliary data construction 25 outputs auxiliary data stream 26.

Depending upon its content, auxiliary data stream 26, so constructed, can be used to correct or augment the NTSC decoded signal 23, or data stream 26 can be used for any other predetermined purpose. As an alternative to the stand-alone chipset or circuit board manifestation of the present invention illustrated within the dashed box in Figure 12, the invention can be incorporated into MPEG-2 decoder 22, in order that auxiliary data stream 26 is available to correct or augment the MPEG-2 bit stream fields.

The foregoing description of the preferred embodiment of the invention have been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed, and obviously many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the invention and its practical application to thereby enable others skilled in the art to best utilize the invention in various embodiments and with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the claims appended hereto.

WHAT IS CLAIMED IS:

1. A method of embedding auxiliary data into host data compressed by lossy compression ratio methods that use series expansion and quantization techniques comprising the steps of:

creating a duplicate digital compression representation of said host data in terms of intermediate integer indices representing coefficients, said digital compression representation having certain statistical properties;

creating a digital representation of said auxiliary data in the form of a sequence of individual bit values;

evaluating said digital compression representation to determine pairs of integer indices differing by a specified number of units and occurring with similar frequency in said digital compression representation;

replacing individual integer indices in said digital compression representation with values taken from a digital key comprising a schedule of said pairs of integer indices in order to embed individual bit values corresponding to said sequence of individual bit values of said auxiliary data; and

outputting said digital compression representation with said auxiliary data embedded into a file format specified for said compressed data.

2. The method as described in Claim 1 further comprising the step of combining said auxiliary data with predetermined information indicative of the presence of said auxiliary data, its file name, and file size, said step to be performed after the step of digitizing said auxiliary data.

3. The method as described in Claim 1 further comprising the step of equalizing said statistical properties of said digital compression representation for the purpose of improving said lossy compression ratio methods.

4. The method as described in Claim 1, wherein said digital compression representation originates from a color image compressed with the JPEG or WSQ algorithm, and their derivative compression representations.

5. The method as described in Claim 1, wherein said digital compression representation originates from a black and white image compressed with the JPEG or WSQ algorithm, and their derivative compression representations.

6. The method as described in Claim 1, wherein said digital compression representation originates from a television or video disc signal compressed with the MPEG and DCT-based algorithms, and their derivative compression representations.

7. The method as described in Claim 1, wherein said digital compression representation originates from digital audio represented by lossy compression representations.

8. The method as described in Claim 1, wherein said digital compression representation originates from X-ray, CT-scan, or Magnetic Resonance Imaging data.

9. The method as described in Claim 1, wherein said digital compression representation originates from personal security and identification information.

10. The method as described in Claim 1, wherein said digital compression representation originates from fingerprint images.

11. The method as described in Claim 1, wherein said digital compression representation originates from images made with a camera producing digital images.

12. A method of constructing embedded a quantity of auxiliary data from a machine readable lossy digital compression representation containing integer indices comprising the steps of:

creating a look-up table defining a correlation between decoded integer indices from said lossy digital compression representation and elements of a key-pair table;

matching said decoded integer indices from said lossy digital compression representation with entries in said look-up table, for determining correspondence of said integer indices from said lossy digital compression representation with said elements in said key-pair;

constructing said auxiliary data according to said correspondence in said look-up table between said integer indices from said lossy digital compression representation and an element in said key-pair table; validating the content and correctness of said auxiliary data by examining header data constructed from the correspondence between said integer indices and said key-pair values; and

interpreting said auxiliary bits as data unrelated to said lossy compressed data.

13. The method as described in Claim 12, wherein said auxiliary data consist of digital text.

14. The method as described in Claim 12, wherein said auxiliary data consist of script or code intended for execution on a network client or server machine.

15. The method as described in Claim 12, wherein said auxiliary data consist of motion vector data or script used in the reconstruction of a digital motion picture.

16. The method as described in Claim 12, wherein said auxiliary data consist of text or digital audio data used for subtitles or language translation of digital motion picture audio.

17. The method as described in Claim 12, wherein said auxiliary data consist of information used to correct degraded, or to decode scrambled image data, for the purpose of controlled service delivery.

18. The method as described in Claim 12, wherein said auxiliary data consist of additional or supplemental digital imagery.

19. The method as described in Claim 12, wherein said auxiliary data consist of personal identification information.

20. The method as described in Claim 12, wherein said auxiliary data consist of medical record or diagnostic information.

21. The method as described in Claim 12, wherein said auxiliary data consist of a portion of the said original lossy compressed data.

22. The method as described in Claim 12, wherein said auxiliary data consist of encrypted information.

23. The method as described in Claim 12, wherein said auxiliary data consist of information transmitted in the space of said lossy compressed representation afforded by the existence of a correspondence between said integer indices and said pair key table.

24. Apparatus for embedding auxiliary data into individual frames of host data having integer indices of certain values and frequencies of occurrence compressed by lossy compression ratio methods that use series expansion and quantization techniques comprising:

buffer storage means receiving said individual frames of host data for entropy decoding, modifying and momentarily storing said integer indices of said individual frames of host data ,entropy coding said modifications to said integer indices of said individual frames of host data, and outputting said entropy coded modifications to said integer indices of said individual frames of host data;

histogram analysis means receiving said entropy decoded integer indices of said individual frames of host data for processing a statistical relationship between said frequency of occurrence and said value of said integer indices of said individual frame of

host data identify embedding pair candidates in said individual frames of host data, and outputting said embedding pair candidates;

key-pair table means receiving said embedding pair candidates for creating a key-pair table for each of said individual frames of host data, and outputting said embedding pair candidates as a randomized table;

compression embedding means receiving said embedding key pair table, said integer indices from said individual frames of host data retained in said buffer storage, and said auxiliary data for embedding said auxiliary data and said key-pair table into said individual frames of host data and outputting an embedded stream of individual frames of host data.

25. The apparatus as described in Claim 24 wherein said buffer storage means, said key-pair table means, and said compression embedding means are contained within a chipset.

26. The apparatus as described in Claim 24 wherein said buffer storage means, said key-pair table means, and said compression embedding means are implemented in circuit board circuitry.

27 Apparatus for constructing auxiliary data and a key-pair table embedded into individual frames of host data compressed by lossy compression ratio methods that use series expansion and quantization techniques comprising:

look-up table means receiving said key-pair table from said individual frames of host data for extracting said key-pair table and outputting a key-pair index corresponding to each of said integer indices from said individual frames of host data in a buffer storage; and

auxiliary data construction means receiving said key pair table for each of said individual frames of host data and said integer indices from said individual frames of host data stored in said buffer storage for using said key pair to construct said auxiliary data from said individual frames of host data and outputting an auxiliary data bit stream.

28. The apparatus as described in Claim 27 wherein said look-up table means and said auxiliary data construction means are contained within a chipset.

29. The apparatus as described in Claim 27 wherein said look-up table means and said auxiliary data construction means are implemented in circuit board circuitry.

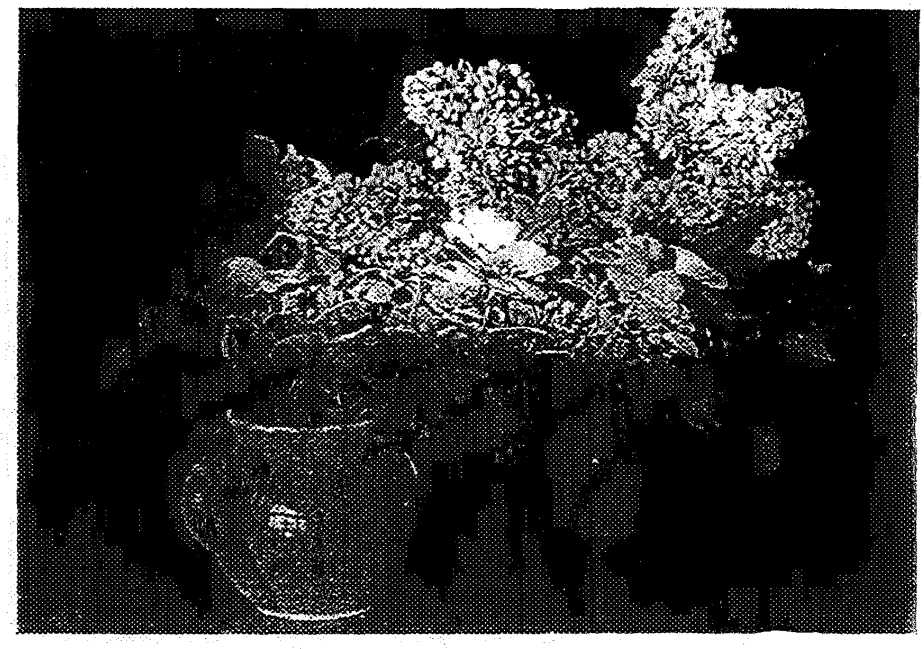


FIGURE 1

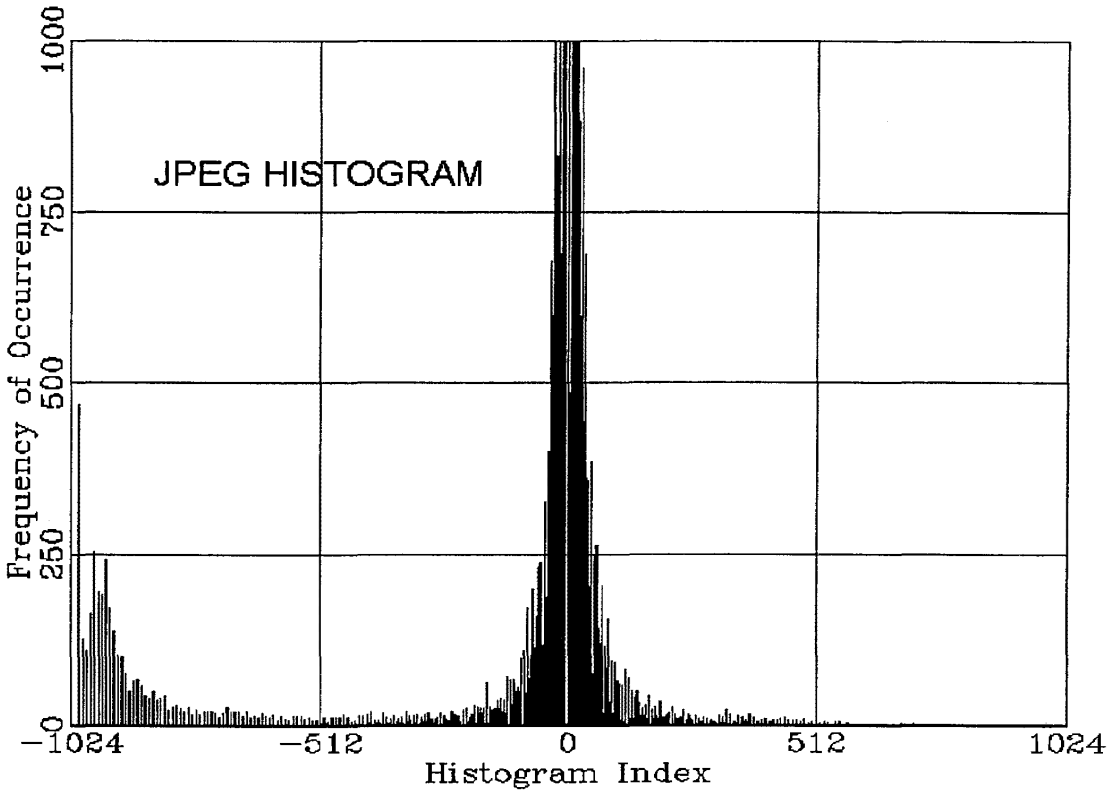

JPEG HISTOGRAM
Frequency of Occurrence
0
250
500
750
1000
−1024
−512
0
512
1024
Histogram Index

FIGURE 2

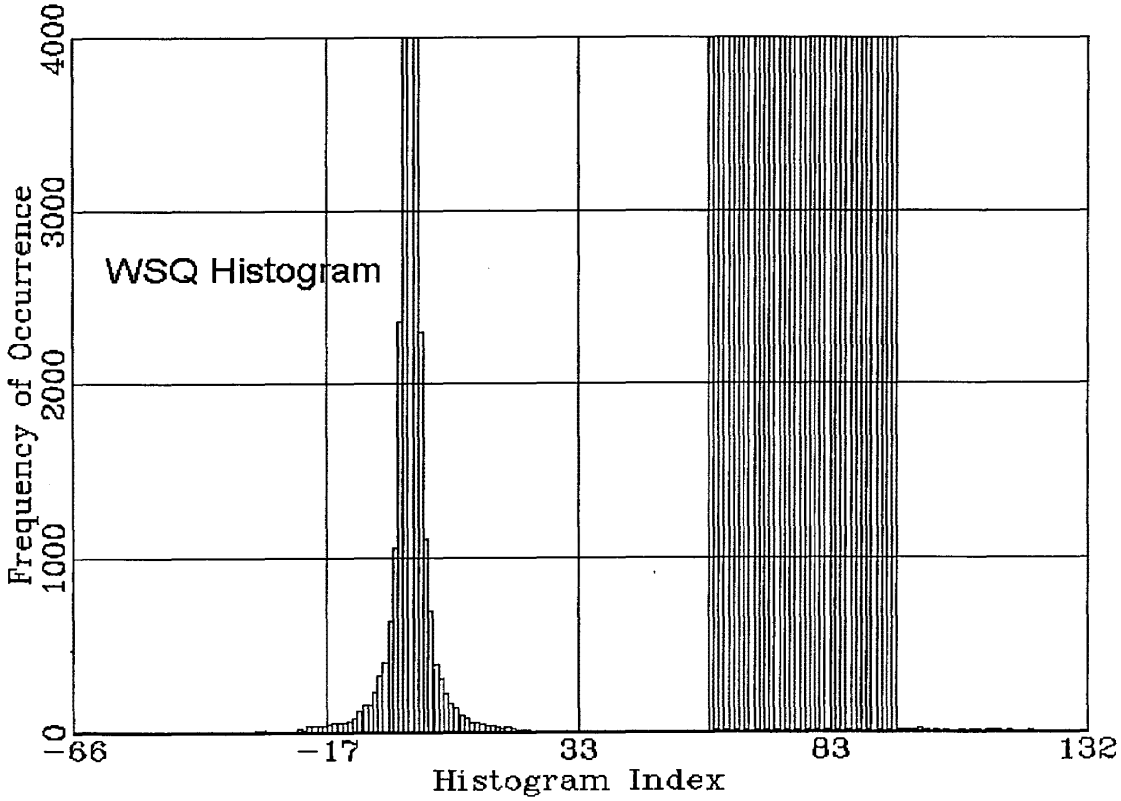

WSQ Histogram
Frequency of Occurrence
0
1000
2000
3000
4000
-66
-17
33
83
132
Histogram Index

FIGURE 3

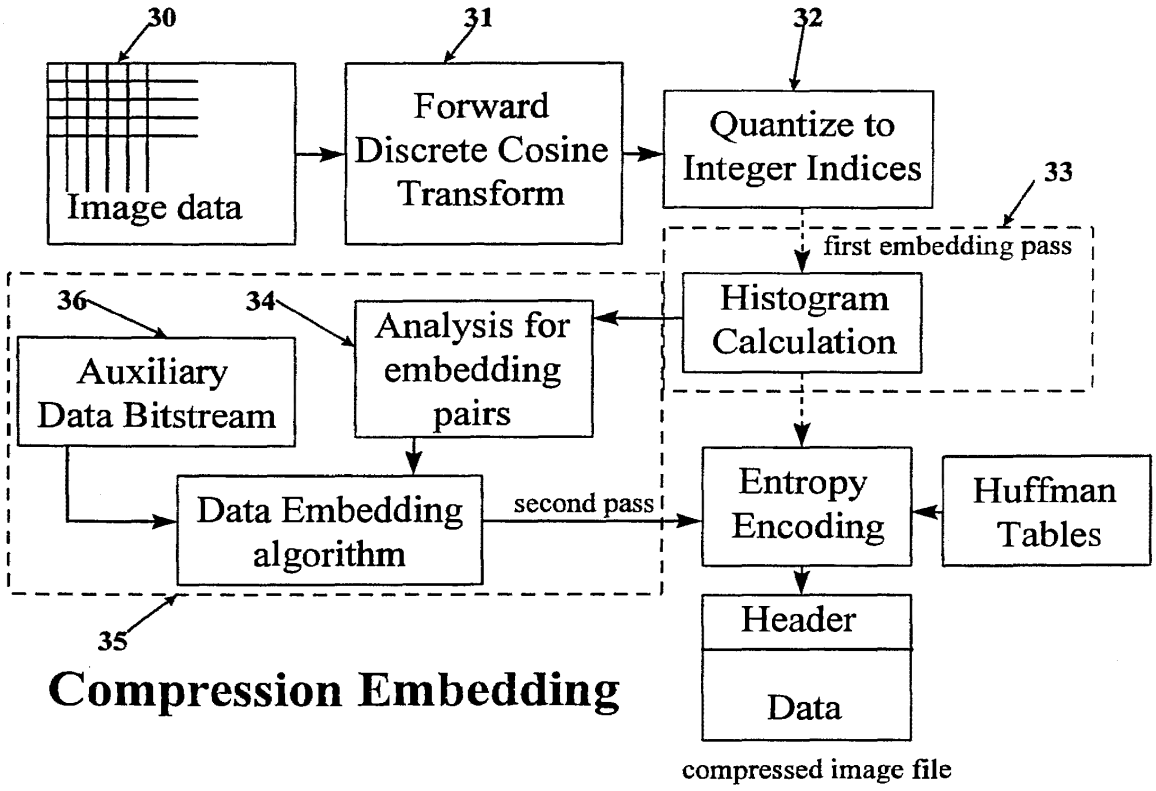

30
31
32
33
Image data
Forward Discrete Cosine Transform
Quantize to Integer Indices
first embedding pass
Histogram Calculation
36
34
Auxiliary Data Bitstream
Analysis for embedding pairs
Data Embedding algorithm
second pass
Entropy Encoding
Huffman Tables
Header
Data
35
Compression Embedding
compressed image file

FIGURE 4

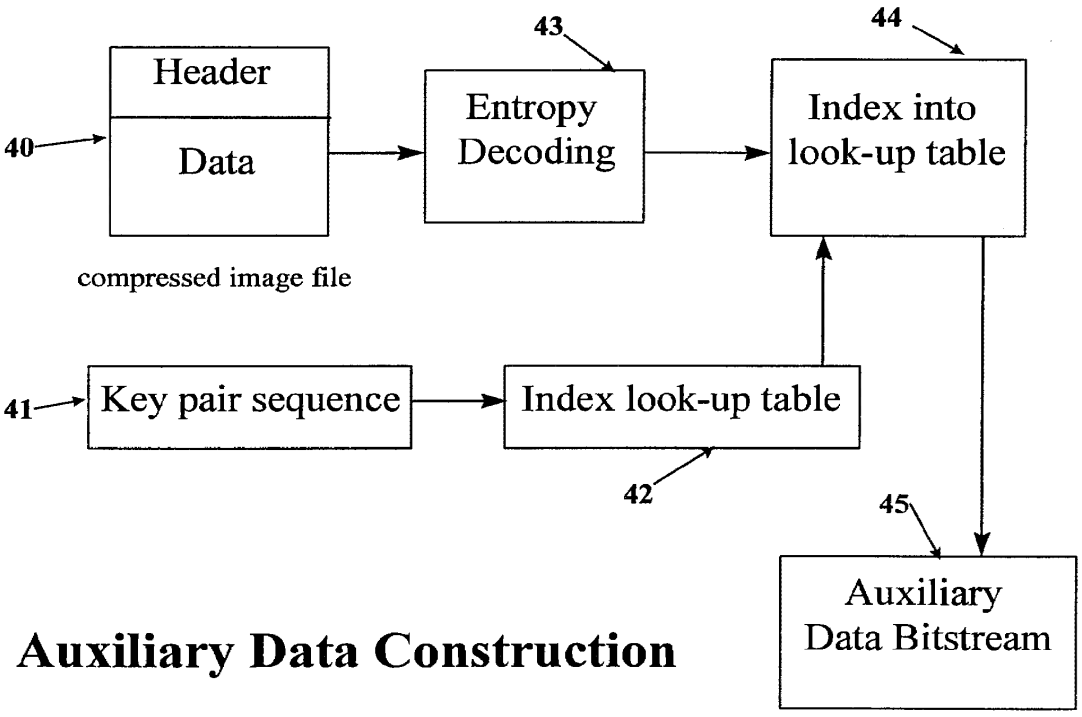

Header
Data
40
compressed image file
43
Entropy Decoding
44
Index into look-up table
41
Key pair sequence
Index look-up table
42
45
Auxiliary Data Bitstream
Auxiliary Data Construction

FIGURE 5

```
/*****************************************************************************************
* JHISTGM.C  Code module to process the histogram data to select key
*            pairs for use in
*            the compression embedding method.
*
* ORIGIN:  Derived from the Compression Embedding application code.
*
* Copyright (c) 1994-1996.  M. T. Sandford II and the University of California.
*     All Rights Reserved.
*
* Version 1.10   10-15-96
*****************************************************************************************/


#include <stdlib.h>
#include <stdio.h>
#include <string.h>

#define H_TABLE_SIZE 2048              /* range of the quantizer output (+/- 1023) */
#define MAXPAIRS 256       /* maximum number of pairs permitted for the key */
#define MINVAL -1024       /* minimum value from quantizer output */
#define HISTLIMIT  3                              /* low-frEquation limit for histogram
entries (+/- limit) */

struct PAIRS {
     short i;
     short j;
     unsigned long count;
     };


/* function prototypes */
void p_sort(struct PAIRS *pair, int no_pair);
void jumble(int *index, int npts);
int duplicate (int nopairs, struct PAIRS *pair);
void jhistgm(long *hist_table, struct PAIRS *pair,int *no_pairs);
void scramble(int no_pairs, struct PAIRS *pair);
extern unsigned long GetAuxFileSize(void);
extern unsigned short getrepwidth(unsigned long size);
```

FIGURE 6

```
/*****************************************************************************************
 * JHISTGM:  routine to process the histogram table and to determine a noise key
 *
 *    INPUT:                                    hist_table, pointer to unsigned long
histogram data
 *
 *    OUTPUT:   *pair[],    values of the pairs stored in a structure array
 *
 *    RETURN:   nothing

*****************************************************************************************
*/

void jhistgm(long *hist_table, struct PAIRS *pair,int *no_pairs)  {
int j;
int iloop;
long lsum;
long lavg;
long ldiff;
unsigned long file_size=0L;
/*    Process histogram to select embedding pairs */
 j = 0;
 for(iloop=0;iloop<H_TABLE_SIZE;iloop++)     {
     if(hist_table[iloop]==0 || abs(iloop+MINVAL) < HISTLIMIT)  {  //skip zero entries
& avoid low frEquation
                                                iloop += 1;
                                                continue;
                                                }
     lsum = hist_table[iloop]+hist_table[iloop+1];
     lavg = lsum/2L;
     ldiff = hist_table[iloop]-hist_table[iloop+1];
     ldiff = labs(ldiff);
     if(ldiff < lavg) {   /* Difference less than avg. for the pair */
                                                pair[j].i = iloop+(int)MINVAL;
                                                pair[j].j = iloop+(int)MINVAL+1;
                                                pair[j].count = (unsigned long)lsum;
                                                j++;
                                                iloop+=2;
                                                if(j==MAXPAIRS)break;
                                                }
     }
```

FIGURE 6

```
  lsum = 0L;
  *no_pairs = duplicate(j,pair);  /* remove duplicates (there should not be any) */
  for (iloop=0;iloop<*no_pairs;iloop++)  {
     if(pair[iloop].i==pair[iloop].j)break;
     lsum += pair[iloop].count;

#ifdef PROGRESS_REPORT
     fprintf(stderr,"\npair[%3d] %4d %4d %5ld", iloop,\
                                                  pair[iloop].i, pair[iloop].j,
pair[iloop].count);
#endif
  }

  // check the embedding space against the amount of auxiliary data
  file_size = GetAuxFileSize();
  fprintf(stderr,"\n%d pairs located. Total embedding space = %ld bytes", *no_pairs,
lsum/8L);
  if(file_size*8L > (unsigned long)lsum)  {
     fprintf(stderr,"\nAuxiliary file size = %ld bytes", file_size);
     *no_pairs = 0;
     }

  // reduce key to the minimum size needed to embed the file
  for(iloop=0;iloop<*no_pairs;iloop++)  {
     if(lsum-pair[iloop].count >= file_size*8L + getrepwidth(file_size) + 5)  {
                                          lsum -= pair[iloop].count;
                                          pair[iloop].count = 0L;       // throw out this
pair
                                          }
     }
  *no_pairs = duplicate(*no_pairs,pair);   // remove discarded pairs

  scramble(*no_pairs,pair);                        // mix up the pairs to form a random
key
  lsum = 0L;
  for(iloop=0;iloop<*no_pairs;iloop++)
     lsum += pair[iloop].count;
  if((unsigned long)lsum >= file_size*8L + getrepwidth(file_size) +5)
     fprintf(stderr,"\n%d byte key",*no_pairs*2);
  return;
}
```

FIGURE 6

```
        /*    DUPLICATE:  Routine to remove entries containing duplicate
                          histogram values in the PAIRS structure
 *      INPUT:            no_pairs, integer no. of pairs in the pixel pair
                          table
 *                        pixpairs, table of PAIRS structures
 *      RETURN:           new value for no_pairs (0 if no entries exist)
 *      AUTHOR:     Copyright (c) 1994-95, M. T. Sandford II
 *                                                Univ. of California, Los Alamos
National
                          Laboratory
 ***************************************************************************/
#include <stdlib.h>

struct PAIRS {          /* structure of pallet pair data entries */
     int i;
     int j;
     unsigned long count;
     };
int duplicate (int nopairs, struct PAIRS *pair)  {
int i;       /* counters */
int j;
int k=0;
if(nopairs == 0)return k;                    /* return if nothing to do */
p_sort(pair,k);                              /* sort pairs by frequency of occurrence */
for(i=0;i<nopairs;i++)                       {
     if(pair[i].count==0L)continue;
     for(j=0;j<nopairs;j++)                  {
          if(j==i)continue;
          if(pair[j].count==0)continue;
          if(pair[j].i == pair[i].i ||
            pair[j].i == pair[i].j ||
            pair[j].j == pair[i].i ||
            pair[j].j == pair[i].j)  {
               if(pair[j].count < pair[i].count)
                    pair[j].count = 0;
               else {
                                             pair[i].count = 0;
                                             break;
                                             }
               }
          }
     }
```

FIGURE 7

```
for(i=0;i<nopairs;i++) { /* remove null entries from pair table */
      j = i+1;
      while(pair[i].count == 0) {
                                          for(k=j;k<nopairs;k++)
                                          pair[k-1] = pair[k];
                                          nopairs--;
                                          if(nopairs==0) break;
            }
     if(nopairs==0)break;
     }
return i;
}
```

FIGURE 7

```
/*****************************************************************************************
*
* SCRAMBLE.C:  Routine to scramble the pair order to a random sequence
*
* INPUT:      no_pairs, integer no. of pairs to scramble
*             pair, pointer to table of structures to scramble
*
* RETURNS:    nothing
*
* OUTPUT:     pair, pointer to the scrambled table of pair structures
*
* AUTHOR:     M. T. Sandford II, 6 Oct. 1994 * Version 1.0
* Copyright © 1996 The University of California and M. T. Sandford II
* All Rights Reserved.

*****************************************************************************************
/
void scramble(int no_pairs, struct PAIRS *pair) {
   int i;                                /* loop counter */
   int *index=NULL;                      /* scrambled index values */
   struct PAIRS *temp_pair=NULL;   /* temporary pair structure table */

   index = (int *)malloc(no_pairs*sizeof(int));
   temp_pair = (struct PAIRS *)malloc(no_pairs*sizeof(struct PAIRS));
   if(index==NULL || temp_pair==NULL) {
     if(index)free(index);
     if(temp_pair)free(temp_pair);
     fprintf(stderr,"\nJumble memory allocation failed!");
     return;   /* no scrambling performed */
     }
   jumble(index,no_pairs);
   for(i=0;i<no_pairs;i++) {
     temp_pair[i].i = pair[index[i]].i;
     temp_pair[i].j = pair[index[i]].j;
     temp_pair[i].count = pair[index[i]].count;
     }
   memmove(pair,temp_pair,no_pairs*sizeof(struct PAIRS));
   free(index);
   free(temp_pair);
```

FIGURE 8

```
   // now scramble the parity of the entries in the pair tables
   for(i=0;i<no_pairs;i++) {
     int temp;
     temp = rand();
     if(temp > RAND_MAX/2) {
                                          temp = pair[i].j;
                                          pair[i].j = pair[i].i;
                                          pair[i].i = temp;
                                          }
                                          }
   return;
}
/*****************************************************************************************
**
 * JUMBLE.C:  Routine to jumble a table of indices using pseudo-random
 *            numbers seeded from the PC clock
 *
 * INPUT:     index, pointer to a table of jumbled integers
 *          npts,  integer no. of entries in the index table
 *
 * RETURN:    nothing
 *
 * OUTPUT:    returns a jumbled table of integers
 *
 * AUTHOR:    M. T. Sandford II, 5 Oct. 1994, following the method
 *          preferred by T. Handel
 *****************************************************************************************/
void jumble(int *index, int npts) {
int i;
float fi;
struct POINTS {
   float gamma;
   int i;
   } *pts;
pts = malloc(sizeof(struct POINTS)*npts);
for (i=0;i<npts;i++) {
   pts[i].i = i;
   pts[i].gamma = (float)rand()/(float)RAND_MAX;
   }
qsort( (void *)pts, (size_t)npts, sizeof(struct POINTS),
                                          index_compare);
```

FIGURE 8

```
for(i=0;i<npts;i++)  {
      index[i] = pts[i].i;
/*      printf("\ni,index[i] %d %d", i, index[i]); */
      }
if(index[0]==0)  {
   fi = (float)rand()/(float)RAND_MAX;
   fi *= (float)(npts-1)+1.0f;
   index[0] = index[(int)fi];
   index[(int)fi] = 0;
   }
free(pts);
}
```

FIGURE 8

```
/*****************************************************************************
 * JEMBED.C  Code module to perform embedding into the quantizer indices
 *
 * Author:  M. T. Sandford II, Sept. 4, 1996.  Version 1.10
 *
 * Copyright (c) 1994-1996.  M. T. Sandford II and the University of California
 *   All Rights Reserved.
 *
*****************************************************************************/
#include <stdio.h>
#include <stdlib.h>
#include <memory.h>

#define MAXPAIRS 256                    /* maximum no. of pairs */
#define MAXSIZE  2049                   /* maximum no. of indices */
#define MINVAL  -1024      /* minimum index value */

/*****************************************************************************
 * Embed_Data_Block:  Routine to embed data into a block of integers using
 *                    the pairs in the structure pair.  This code was re-
 *                    written from the original version, to use table look-up
 *                    for the embedding values.
 *
 *   INPUT:             buffer,   pointer to the block of integers
 *   ibuf,              integer no. of integers in the block
 *
 *   Note:  The following are determined by reading the keyfile
 *                                  pair,    pointer to index pair structures
 *                                  no_pairs, number of pair structures
 *
 *   RETURN:                        nothing
 *
*****************************************************************************/

static int ptable[MAXSIZE];                 /* table of pairs */
static int ptable_filled = 0;               /* flag to fill the table */
static unsigned long embed_count=0L;  /* total number of embedded bits */
```

FIGURE 9

```
static struct PAIRS {                    /* structure of pallet pair data entries */
    int i;
    int j;
    unsigned long count;
    }pair[MAXPAIRS];
static int no_pairs;

extern short bitgetbit(void);        /* Derek Upham's data code */
extern FILE *fpKeyFile;                                          /* pointer to the
pair key file */

void Embed_Data_Block(short *buffer,int ibuf)  {
short index;
int i;
int j;
int k;
size_t inbytes=0;
if(!ptable_filled)  {
    fseek(fpKeyFile,0L,SEEK_SET);    // retrieve the pair values from the keyfile
    no_pairs = 0;
    for(i=0;i<MAXPAIRS;i++)  {
                                     k = sizeof(int)*fread(&pair[i].i,sizeof(int),1,
fpKeyFile);
                                     if(k==0)break;
                                     inbytes += k;
                                     k = sizeof(int)*fread(&pair[i].j,sizeof(int),1,
fpKeyFile);
                                     if(k==0)break;
                                     inbytes += k;
                                     no_pairs++;
                                     }
    pair[no_pairs].i = pair[no_pairs].j = 0;
    pair[no_pairs].count = 0L;
  fclose(fpKeyFile);                                    // all done with the
keyfile (it could be compressed now)
  fpKeyFile = NULL;
```

FIGURE 9

```
   for(k=0;k<MAXSIZE;k++) ptable[k] = -1;
     for(k=0;k<no_pairs;k++)  {
                                        index = pair[k].i - MINVAL;
                                        ptable[index] = k;
                                        index = pair[k].j - MINVAL;
                                        ptable[index] = k;
                                        }
      ptable_filled = 1;                                    // the key lookup table
is filled & can be used
   }


for(j=0;j<ibuf;j++)                     {           // loop over each value in the
buffer
                                        index = buffer[j]-MINVAL;
                                        k = ptable[index];
                                        if(k>=0) {          // does the value match
with a key-pair element?
                                                embed_count++;
                                                if ((i=bitgetbit()) != -1)  {
                                                        if(i) index = pair[k].j;
                                                        else  index = pair[k].i;
                                                        buffer[j] = index;
                                                        //buffer[j] = 35;               //
intentionally corrupt the element for display purposes
                                                        }
                                                }
                                        }
return;
}
```

FIGURE 9

```
/*****************************************************************************************
*   ExtractDataBlock:  Routine to extract data from a block of integers using
*                                        the pairs in the structure pair.  This code
was re-written from the
*                                        original version, to use table look-up for
the embedding values.
*
*   INPUT:                               buffer,   pointer to the block of integers
*                                              ibuf,    integer no. of integers in the
block
*
*   Note:  The following are determined by reading the keyfile
*                                              pair,    pointer to index pair
structures
*                                              no_pairs, number of pair structures
*
*   RETURN:                              nothing
* Version 1.10 10/15/96
* Copyright © 1996 M. T. Sandford II and The University of California
* All Rights Reserved.
*****************************************************************************************/

static int ptable[MAXSIZE];                                    /* table of pairs */
static int ptable_filled = 0;                          /* flag to fill the table */
static unsigned long embed_count=0L;  /* total number of embedded bits */
static int no_pairs;
static int alldone=0;                                  /* flag for completion of
extraction */

extern struct PAIRS {                                  /* structure of pallet pair data entries
*/
    int i;
    int j;
    unsigned long count;
    }*pair;

extern int bitsetbit(unsigned char value);  /* Derek Upham's data code */
extern unsigned long GetFileSize(void);   /* routine to return extracted file size */
extern FILE *fpKeyFile;                        /* pointer to the pair key file */
```

FIGURE 10

```
void ExtractDataBlock(short *buffer,int ibuf) {
short index;
int i;
int j;
int k;
size_t inbytes=0;
unsigned long fsize = 0;

if(alldone) return;                                    // nothing left to do

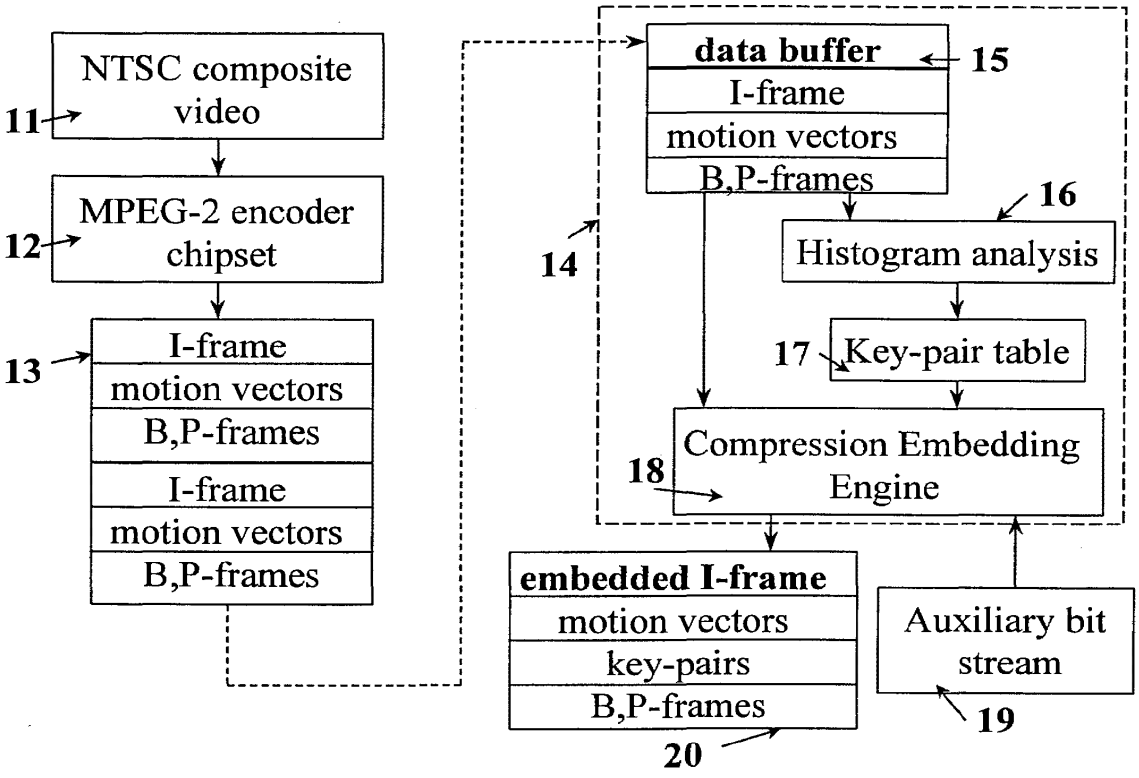
if(!ptable_filled) {
    //fpKeyFile = fopen("keyfile", "rb");              // retrieve the pair values from the keyfile
    no_pairs = 0;
    for(i=0;i<MAXPAIRS;i++) {
                                                       k = sizeof(int)*fread(&pair[i].i,sizeof(int),1,
fpKeyFile);
                                                       if(k==0)break;
                                                       inbytes += k;
                                                       k = sizeof(int)*fread(&pair[i].j,sizeof(int),1,
fpKeyFile);
                                                       if(k==0)break;
                                                       inbytes += k;
                                                       no_pairs++;
                                                       }
    pair[no_pairs].i = pair[no_pairs].j = 0;
    pair[no_pairs].count = 0L;
  fclose(fpKeyFile);                                                    // all done with the keyfile
  fpKeyFile = NULL;
  for(k=0;k<MAXSIZE;k++) ptable[k] = -1;
    for(k=0;k<no_pairs;k++) {
                                                       index = pair[k].i - MINVAL;
                                                       ptable[index] = k;
                                                       index = pair[k].j - MINVAL;
                                                       ptable[index] = k;
                                                       }
    ptable_filled = 1;                                                  // the key lookup table is filled &
can be used
  }

for(j=0;j<ibuf;j++)                                    {                // loop over each value in the
buffer
                                                       index = buffer[j]-MINVAL;
                                                       k = ptable[index];
                                                       if(k>=0) {                  // does the value match
with a key-pair element?
                                                       if(pair[k].i == buffer[j]) i = bitsetbit(0x00);
                                                       else i = bitsetbit(0x01);
```

FIGURE 10

```
                                        if(i==-1) {
                                                alldone = 1;
                                                fsize = GetFileSize();
                                                fprintf(stderr,"\n%6ld header
bytes extracted", embed_count/8L - fsize);
                                                fprintf(stderr,"\n%6ld   data
bytes extracted\n", fsize);
                                                fflush(stderr);
                                                }
                                        embed_count++;
                                        }
                                }
return;
}
```

FIGURE 10


NTSC composite video
11
MPEG-2 encoder chipset
12
I-frame
motion vectors
B,P-frames
I-frame
motion vectors
B,P-frames
13
14
data buffer
15
I-frame
motion vectors
B,P-frames
16
Histogram analysis
17
Key-pair table
18
Compression Embedding Engine
embedded I-frame
motion vectors
key-pairs
B,P-frames
20
Auxiliary bit stream
19

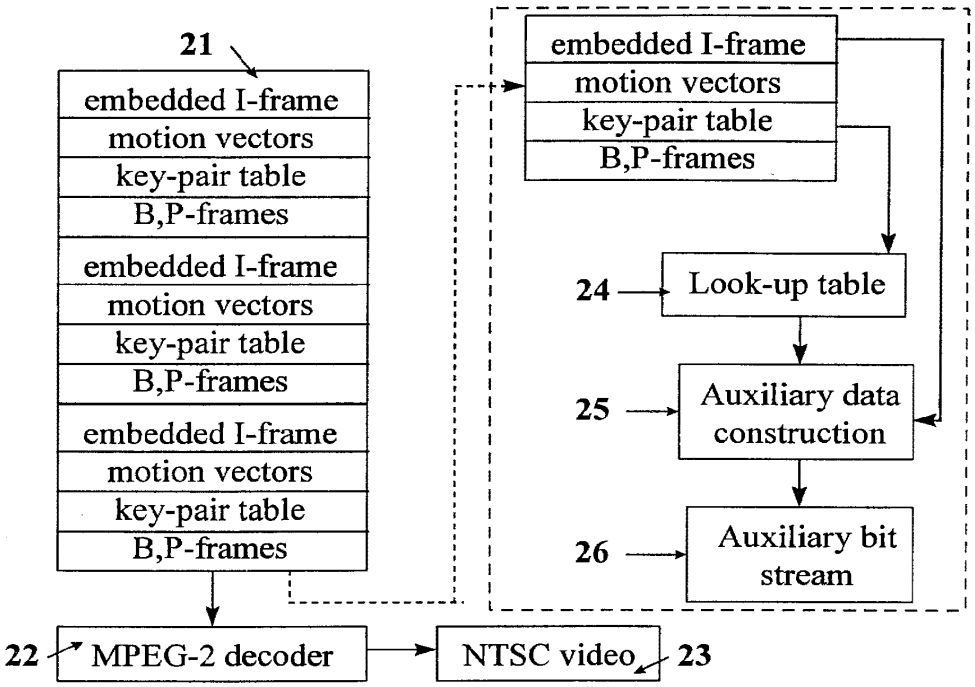

21
embedded I-frame
motion vectors
key-pair table
B,P-frames
embedded I-frame
motion vectors
key-pair table
B,P-frames
embedded I-frame
motion vectors
key-pair table
B,P-frames
22
MPEG-2 decoder
NTSC video
23
embedded I-frame
motion vectors
key-pair table
B,P-frames
24
Look-up table
25
Auxiliary data construction
26
Auxiliary bit stream

FIGURE 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/23291

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06K 9/00
US CL :Please See Extra Sheet.
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. : 364/715.02; 348/416; 235/382, 494; 358/426, 434; 382/232, 233, 236, 239, 243, 250, 254

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)

APS
search terms: lossy, compression, integer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,636,292 A (RHOADS) 03 June 1997, column 3, lines 1-67.	1-29

☐ 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 23 FEBRUARY 1998	Date of mailing of the international search report 27 APR 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 LEO BOUDREAU Telephone No. (703) 308-7595

Form PCT/ISA/210 (second sheet)(July 1992)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/23291

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

364/715.02; 348/416; 235/382, 494; 358/426, 434; 382/232, 233, 236, 239, 243, 250, 254

Form PCT/ISA/210 (extra sheet)(July 1992)★

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G11B 23/28, 23/36, 23/40	A1	(11) International Publication Number: WO 00/36605
		(43) International Publication Date: 22 June 2000 (22.06.00)

(21) International Application Number: PCT/SG98/00104

(22) International Filing Date: 11 December 1998 (11.12.98)

(71) Applicant *(for all designated States except US)*: KENT RIDGE DIGITAL LABS [SG/SG]; 21 Heng Mui Keng Terrace, Singapore 119613 (SG).

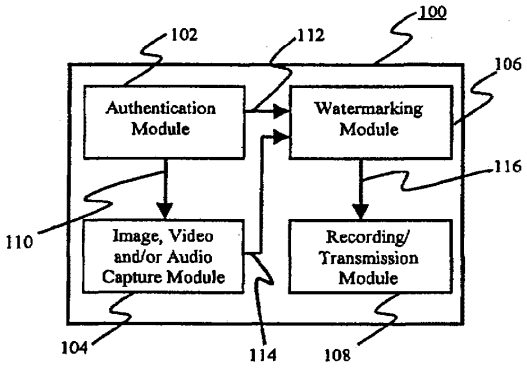
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: WU, Jian, Kang [CN/SG]; Blk 51 Teban Gardens Road, #06–605, Singapore 600051 (SG). NARASIMHALU, A., Desai [IN/SG]; 103 Clementi Road, #03–01, Kent Vale, Singapore 129788 (SG). LO, Sheng [SG/SG]; Blk 444, Jurong West Avenue 1, #11–774, Singpaore 640444 (SG). LEBRUN, Jean–Luc [FR/SG]; 10G Braddell Hill, #23–27 Braddell View, Singapore 579726 (SG).

(74) Agent: SPRUSON & FERGUSON PTE LTD.; 51 Bras Basah Road, #02–03 Plaza by the Park, Singapore 189554 (SG).

(81) Designated States: GB, SG, US.

Published
With international search report.

(54) Title: METHOD AND DEVICE FOR GENERATING DIGITAL DATA WATERMARKED WITH AUTHENTICATION DATA



(57) Abstract

An apparatus (100), method and computer program product for generating an authenticated audio, image and/or video signal (116) is disclosed. The apparatus or recording device (100) includes an authentication module (102), an audio, image and/or video capture module (104), and a watermarking module (106). The apparatus can be a digital camera, digital video camera, or a digital audio recording device. The authentication module (102) checks if the operator is authorized to use the apparatus (100) and if so generates authentication information (112). Biometrics data such as a fingerprint, iris, voice and/or face recognition can be used for authentication. If authorized, the capture module (104) generates an audio, image and/or video signal (114). A watermarking module (106) embeds the authentication information (112) in the media signal (114) to provide the authenticated output signal (116). The watermarking is built into the recording device (100) and is carried out on–the–fly. The media signal can be watermarked with GPS data and/or annotation.

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		

METHOD AND DEVICE FOR GENERATING DIGITAL DATA WATERMARKED WITH AUTHENTICATION DATA

FIELD OF THE INVENTION

The present invention is directed to the field of recording digital audio, image and/or video signals and, in particular, to a method and apparatus for embedding information in digital audio, image and/or video signals.

BACKGROUND

The subsistence of copyright in artistic works is a significant and valuable right rewarding artistes for their original, creative efforts. Amongst other things, the subsistence of copyright in an artistic work allows a copyright owner to advantageously commercially exploit their work and also to control the use and treatment of such artistic works by others. The existence of copyright is particularly important in relation to artistic works in fields such as photography, music and film.

In conventional photography and other image acquisition processes, claims of ownership in photographs and similar image recordings are typically indicated by manually labeling the back of the photographs with details of the owner. Alternatively, stickers or rubber stamps may be used to mark the photographs. However, such methods do not provide incontrovertible or substantially incontrovertible evidence of ownership of the artistic work by the owner. For example, a false claim of ownership can be made on unmarked materials owned by another, can be defaced or erased, or can be overwritten with false markings of another claimant.

In film and video recordings, ownership rights are frequently made by adding details of the owner in a header and/or a trailer portion of the recording. For audio recordings, ownership details are normally indicated on the recording media (e.g., CD-ROM, tape, etc.) or packaging. However, ownership indicia are capable of being easily removed or altered from the recordings or packaging.

With the widespread advent of digital recording technology, artistic works can be readily duplicated and distributed worldwide immediately by communication channels like the Internet, Intranets, and satellite communications. Further, such digital artistic works are readily susceptible of unauthorised modification and tampering. The recording of an artistic work in the digital domain exacerbates the problems of establishing ownership of copyright in an artistic work. Several techniques have been attempted to address this issue.

United States Patent No. 5,513,260 discloses a method and apparatus that attempts to provide copyright protection for recording media such as compact discs (CDs) using encryption. In particular, a combination of symmetrical and asymmetrical data encryption is used to permit a reproduction device to handle either copy-protected or non-copy-protected media. The technique encrypts the digital recording on a recording media. However, the system does not directly relate the artistic work contained in the recording with the copyright owner, and a digital recording once decrypted can be copied or modified without any protection for the copyright owner.

United States Patent No. 4,890,319 discloses a subscription television system for distributing copyrighted program material to subscribers. The system has a transmitter with a data-insertion circuit for inserting a control bit in a transmitted signal, which comprises other control data and the copyrighted program material. A receiver in the system includes a memory for storing a pre-assigned subscriber identification. Upon receipt and identification of the control bit at the receiver, the receiver inserts a subscriber identification into the program material. An unauthorized copy of the program material may be determined since it includes the subscriber identification. However, again, the system does not directly relate the artistic work itself contained in the recording with the copyright owner, and a party familiar with the system can defeat the system by appropriate processing to remove the subscriber identification.

The foregoing systems are disadvantageous in that they fail to uniquely relate the content of the artistic work itself with the owner in a manner that effectively prevents

tampering. Further, the systems cannot ensure that the recordings to which the techniques are applied are the property of the party asserting ownership.

SUMMARY

The aspects of the invention are directed to ameliorating or overcoming one or more disadvantages of conventional systems including those described above. The aspects of the invention are able to do so by requiring authentication data derived from an authorised operator to operate a recording device and providing on-the-fly copyright ownership indicia in a recording, when recording, by watermarking the recording using the authentication data.

In accordance with a first aspect of the invention, a method of generating an authenticated audio, image and/or video signal is disclosed. The method includes the steps of generating an authentication signal, capturing a digital audio, image and/or video signal, and watermarking the digital audio, image audio, image and/or video signal using the authentication signal to provide the authenticated audio, image and/or video signal.

Preferably, the method further includes the steps of: determining if an operator is authorised to generate the authenticated audio, image and/or video signal; and if so, enabling capture of the digital audio, image and/or video signal.

Preferably, the step of generating the authentication signal is performed substantially simultaneously with the step of capturing the digital audio, image and/or video signal. Further, the authentication signal can be derived from biometrics data, a password, user identification data, positioning data, chronological data, data transmitted from an external, remote source and/or data from a removable media.

Optionally, the step of capturing the digital audio, image and/or video signal includes: capturing an analog audio, image and/or video signal; and converting the analog audio, image and/or video signal to the digital audio, image and/or signal.

Also, the watermarking step provides perceptible and/or non-perceptible watermarks. Optionally, the method includes annotating the digital audio, image and/or video signal using text and/or audio data. The annotation can be persistent and/or non-persistent.

In accordance with a second aspect of the invention, an apparatus for generating an authenticated audio, image and/or video signal is disclosed. The apparatus includes: a module for generating an authentication signal; a module for capturing a digital audio, image and/or video signal; and a module for watermarking the digital audio, image and/or video signal using the authentication signal to provide the authenticated, copyrighted audio, image and/or video signal.

Preferably, the apparatus further includes: a module for determining if an operator is authorised to generate the authenticated audio, image and/or video signal; and a module for enabling capture of said digital audio, image and/or video signal in response to determining the operator is authorised.

Preferably, the module for capturing the digital audio, image and/or video signal operates substantially simultaneously with the module for generating the authentication signal. Further, the authentication signal can be derived from biometrics data, a password, user identification data, positioning data, chronological data, data transmitted from an external, remote source and/or data from a removable media.

Optionally, the module for capturing the digital audio, image and/or video signal includes: a module for capturing an analog audio, image and/or video signal; and a module for converting the analog audio, image and/or video signal to the digital audio, image and/or signal.

Also, the watermarking module provides perceptible and/or non-perceptible watermarks. Optionally, the apparatus includes a module for annotating the digital

audio, image and/or video signal using text and/or audio data. The annotation can be persistent and/or non-persistent.

In accordance with a third aspect of the invention, a computer program product having a computer readable medium having a computer program recorded therein for generating an authenticated audio, image and/or video signal is disclosed. The computer program product includes: means for generating an authentication signal; means for capturing a digital audio, image and/or video signal; and means for watermarking the digital audio, image and/or video signal using the authentication signal to provide the authenticated audio, image and/or video signal.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention are described hereinafter with reference to the drawings, in which:

Figure 1 is a block diagram of an apparatus for generating an authenticated audio, image and/or video signal in accordance with a first embodiment of the invention;

Figure 2 is a flowchart illustrating a method of generating an authenticated audio, image and/or video signal in accordance with a second embodiment of the invention; and

Figure 3 is a block diagram of an apparatus for generating an authenticated audio, image and/or video signal in accordance with a third embodiment of the invention;

DETAILED DESCRIPTION

A method, apparatus and computer program product for generating an authenticated audio, image and/or video signal, where the authenticated signal is an audio, image and/or video signal watermarked with authentication data, are described. In the following description of several embodiments, numerous specific details such as particular watermarking techniques are described in order to provide a more thorough

description of those embodiments. It will be apparent, however, to one skilled in the art that the present invention may be practiced without those specific details. In other instances, well-known features such as particular video formats (e.g. MPEG), particular biometrics data, for example, have not been described in detail so as not to obscure the invention.

In broad terms, the embodiments of the invention provide a mechanism for providing a robust, tamper-evident "stamp" of authorship and/or ownership of audio, image and video works. This is done by requiring authentication data to operate an audio, image and/or video-recording device and providing on-the-fly copyright ownership indicia in an audio, image and/or video recording, when recording, by watermarking the recording using the authentication data. The authenticated watermarking is used to verifiably establish the subsistence of copyright ownership of the audio, image and/or video materials.

In the embodiments of the invention, both the generation of authentication data specific to the owner or operator of the recording device and the watermarking are implemented as components of the recording device. Amongst other things, this overcomes disadvantages of the prior art where watermarking might be implemented as an external post-processing procedure on a work downloaded or retrieved from a recording device at one point in time and then watermarked at a later point. In such circumstances, the presence of an original un-watermarked audio, image and/or video work external to the recording device provides opportunities for further disputes in the authenticity of the images. This might occur for example where a third party obtained a copy of the original un-watermarked audio, image and/or video work and watermarked it with data indicating that it was their property. In such circumstances, both the proper owner and the third party would have watermarked copies of the original work with conflicting claims of authorship and/or ownership.

The embodiments of the invention embed watermarking technology directly into the audio, image and/or video acquisition process as a means of protecting intellectual

property rights in the acquired work. In particular, one embodiment directly embeds the watermarking module into the hardware of the recording or acquisition device. Such an arrangement can render every segment of captured media via the recording device to bear the desired digital signature and/or caption embedded by the watermarking module.

For example, when a digital photo or a video segment is taken, immediately there can be potential copyright and annotation issues. Examples of persons affected by such issues include professional journalists and film producers. The embodiments of the invention significantly reduce and potentially eliminate conflicts regarding copyright authorship and ownership if the photo and video, for example, are watermarked with authenticated information specific to the journalist and film producer as soon as they are created. With a properly watermarked photo, the journalist can safely send it to the person's news agent and other news agents with significantly less concern that such persons might successfully assert an improper claim of copyright and/or ownership of the work. Since the audio, image and/or video work is in digital form, it can be easily indexed, stored in a data storage device, and transmitted over a network.

To prevent unauthorized access of the camera/recorder and unauthorized use of data captured by the camera/recorder, an authentication module is included in the camera/recorder to control operation of the camera/recorder. The authentication module may implement any of a number of authentication techniques such as: biometrics data including fingerprints, voice, and face of an authorised operator; a removable smart card containing encoded or encrypted data specific to the authorised operator; a password known by the authorised operator, etc. Alternatively, access data may be transmitted from a remote device such as radio, infrared or other appropriate transmitter acting as a security key of sorts. The authentication module further serves to enforce the authenticity of the recording equipment. The embodiments of the invention can be implemented to render the recording equipment useless in the event of theft, for example.

Optionally, the embodiments of the invention may also incorporate encryption and scrambling techniques, which are widely used in relation to digital photographs, video, and audio to protect them from unauthorized usage. Still further, the embodiments may incorporate an annotation module for annotating an audio, image and/or video work with text and/or audio information, for example. Optionally, the embodiments of the invention implement persistent annotation using watermarking and on-line annotation using voice.

A block diagram of a recording device according to a first embodiment of the invention is depicted in Fig.1. The device 100 for generating an authenticated audio, image and/or video signal includes an authentication module 102, an image, video and/or audio capture module 104, and a watermarking module 106 as its principal features. It also includes a recording/ transmission module 108 for recording and/or transmitting the authenticated audio, image and/or video signal containing embedded watermarks. The authentication module 102 is used to determine whether or not an attempted operator of the device 100 is an authorized user. It is also used to obtain and determine authentication information 112, which is subsequently watermarked in the capture audio, image and/or video work. The capture module 104 can be a type of digital camera, video camera or audio recorder. The watermarking module 106 embeds the authentication information 112 into the digital media 114 to provide the authenticated audio, image and/or video signal 116. Again, this is done to indicate copyright authorship and/or ownership of the audio, image and/or video work.

In particular, the authentication module 102 provides an enabling/disabling signal 110 to the image, video and/or audio capture module 104 dependent upon the results of checking if the attempted operator is authorised to use the device 100. For example, if the authentication module 102 determines that the attempted operator is authorised to operate the device 100, it generates an enable signal 110 which can actuate the image, video and/or audio capture module 104 to generate a relevant signal. Conversely, the authentication module 102 can disable 110 the capture module 104 if the attempted operator is not authorised.

The authentication module 102 protects usage of the device 100 as well as creation of authentication information 112. Authentication can be implemented in any of a number of ways. The simplest is to require the operator to input a password, perhaps using a keypad, to the recording device 100. Another way of implementing authentication is to require the user to swipe an encoded magnetic card through a card reader built in as part of the recording device 100. Alternatively, the device 100 can be adapted to receive an electronically readable card such as a smart card serving as a token that the authentication module 102 can check. Perhaps, the most secure way is to use a device for capturing biometric data from the operator such as fingerprint, facial, or speech recognition. As an example, for the case where the recording device 100 is a digital camera, a transparent button may be used as the button for actuating the digital camera to capture an image in a conventional manner. The authentication module may include a sensor for capturing the fingerprint of the operator when the operator presses the camera actuation button. Alternatively, the sensor may be oppositely disposed in the body of the recording deive, such as at its bottom, where the operator might place a thumb when pressing the actuation button.

Prior to any other processing by the camera, the authentication module 102 can check the captured fingerprint against one or more authorised fingerprints stored in a storage device (e.g. an electronic memory, magnetic storage device, optical storage device,) forming part of the authentication module 102 to determine if the operator is authorised to use the camera. Another implentation may obtain a retinal scan of an eye of the operator as biometric data when the operator looks into the camera sight and presses the actuation button. Still another implementation may use speech recognition in respect of an audio recorder to actuate the recorder where the recorder is voice actuated. As specific details for obtaining biometric data and comparing them with stored data are well known, these details of the authentication module 102 are not set forth in further detail so as not to obscure the invention. Likewise the use of passwords, magnetic cards and electronic cards such as smart cards are well known and therefore these features are not set forth in greater detail.

Authentication carried out by the authentication module 102 can be performed when the operator starts using the recording device 100, and when the operator stops using it for a certain period. Alternatively, the authentication module 102 may require verification of the operator periodically during operation of the recording device 100. For example, for each shut of a digital camera, the authentication module 102, if implemented as an iris-recognition module or a fingerprint-recognition module, can be built in to verify automatically the operator when that person aims the digital camera at a target.

Preferably, default authentication information 112 is loaded each time an authorised operator starts using the recording device 100. Optionally, an editing function is provided to enable the operator to edit authentication information contained in or derived from the authentication module 102. The default authentication information 112 may include one or more of the following: the name of the owner of the recording device 100 or of the authorised operator, the organization relevant to the owner or operator, and the time and date. The foregoing authetication information is merely exemplary. Alone or in combination with other data, it may contain original biometric data such as information derived from the operator's fingerprint. As described hereinafter in relation to another embodiment of the invention hereinafter, the authentication information 112 may optionally include location data identifying the place where the media data is captured. The location may be automatically determined using the Global Position System (GPS).

As yet another example, a recording device 100 according to the first embodiment can be implemented as a high-end digital camera, which is owned by a journalist "John" who is the only authorised user of the camera. In the camera as purchased, a password can be set in the authentication module 102. John can use the password to access the camera 100 initially, change the password to be his fingerprint, and register himself as the only authorised user. He can also set the default authentication information 112 to include his full name, time and location when the picture is taken. The authentication

module 102 can include a small-size, solid-state fingerprint scanner (not shown) that can be well fitted readily to the body of the digital camera 100. When John holds the camera 100 ready to capture an image, his thumb is on the scanner. Without John noticing, when John is holding the camera and attempts to actuate the shutter button, the scanner captures his thumb print and the thumb print is processed by the authentication module 102 to extract minuature points from the scanned image. For detailed information about biometrics authentication, reference is made to Jain, A., Bolle, R., and Pankanti, S., BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers, October 1998. The minuature points can then be matched by the authentication module 102 against ones captured and stored together with his name and other authentication information in a storage device of the capture module 102. The match can take account of the location, type, and orientation of those minuature points. The default authentication information 112 can be retrieved and sent to the watermarking module 106. If the authentication is not successful, operation of the camera shutter in the image capture module 104 is locked or inhibited.

For each individual operation of the recording device 100 or at predetermined instances in a continuous recording interval, the captured media data 114 output by the capture module 104 is watermarked automatically by the watermarking module 106 by embedding one or more watermarks into the media data 114. Preferably, each watermark is a non-perceivable signal. However, the watermarking module 106 can be implemented to embed perceivable watermarks. The embedded signal preferably contains the authentication information the user has edited. Any of a number of watermark techniques for image, audio and video signals may be practiced in the watermarking module 106. Preferably, the particular watermarking techniques to be practiced in the embodiments of the invention possess the following features: non-perceivable, robust, and tamper-proof. By "non-perceivable" is meant that there is no perceivable difference between an original and a watermarked media (i.e., audio, image and/or video signal). In other words, the watermarking process does not affect a predetermined level of humanly perceivable quality of the original media. By "robustness" is meant that an embedded watermark signal is not removable under

media processing and manipulation processes such as filtering, analog-to-digital (A/D) and digital-to-analog (D/A) conversion, and geometric transformations. By "tamper-proof' is meant that the ownership of the media is well-protected against attacks by others.

For additional security, the watermarked media signal can be scrambled/encrypted using a private key generated from the authentication information, for example, or directly from the biometrics data.

As a further optional feature, a database entry can be created in a storage medium of the recording device 100 to keep a record of watermarked media data. For law-enforcement purposes, amongst others, certain registration information contained in the database can be sent to an authority or a public service center, in a manner known to those skilled in the art. Similar techniques are used to register digital signatures via the Internet, for example. This registration information can later be used to verify the authorship and/or ownership of the audio, image and/or video work that has been watermarked with authentication data.

Again with reference to an implementation of the recording device 100 as a digital camera (the following applies equally to digital video and audio recording), after authentication that may be transparent to the operator, John identifies new scenery for image capture and presses the shutter button of the camera 100. Actuation of the button activates capture of a digital photo by the capture module 104 and watermarks the digital photo or image 114 with the authentication information 112 provided by authentication module 102. There are many image watermarking techniques available for such a digital photo application. For an exemplary watermarking technique, reference is made to Cox, I.J., Kilian, J., Leighton, T. and Shamoon, T., Secure Spread Spectrum Watermarking for Multimedia, NEC Technical Report, 95-10. That watermarking technique can be used in this embodiment to convert the authentication information (e.g., the operator's identification) into signal patterns based on the concept of spread spectrum communication. The signal patterns are added to the

original image in the transform domain (e.g., digital cosine transform can be used). By doing so, the embedded watermark signal is spread over the whole image of the digital photo 114. It is therefore difficult to remove the watermark signal using ordinary image processing operations, making it strongly tamper-proof.

Further, the digital photo watermarked with the authentication data 116 output by the watermarking module 106 can be recorded on a storage medium or transmitted to an external location by the recording/transmission module 108.

The recording/transmission module 108 can include storage media such as electronic, magnetic, optical and/or magneto-optical storage media, which can be implemented as removable or non-removable storage media. As an illustrative example, the media can be a removable storage medium such as a floppy disc, which is used in a number of commercial digital cameras. Numerous other media can be practiced without departing from the scope and spirit of the invention. The recording/transmission module 108 can be implemented to transmit the output signal 116 to an external device or location. For example, the output signal 116 can be transmitted by an infra-red transmitter built into the recording device 100 to a corresponding receiver in another device such as a computer. Alternatively, it can be transmitted electrically via an appropriate interface built into the device 100 via one or more conductors to an external device and then to the Internet or an Intranet. The foregoing are merely indicate a few of the many ways of transmitting information between two devices that can be practiced. The watermarked photo 116 can be sent to John's representative so that the photo can be immediately used by various news agents. Preferably, the communication of the photo from the recording/transmission module 108 is via a wireless communication network. Optionally, registration information about the digital photo 116 can also be sent to a service center if necessary.

In the foregoing embodiment of the invention, the functionality of each module 102, 104, 106, and 108 can be implemented as an electronic circuit. Alternatively, at least part of the functionality of each module may be implemented as a computer program

that is carried out by a microprocessor coupled to appropriate storage means, both forming part of the recording device 100. Numerous audio, image and video capture devices are implemented utilising microprocessors and other forms of computer systems. For example, the watermarking module 106 can be implemented entirely as software executing on a microprocessor in the recording device 100. Analogously, the authentication module can be implemented using an appropriate sensing or coupling device to obtain a required external signal or information in conjunction with software executing on a microprocessor to carry out the remaining functionality of the module or a portion thereof.

A flowchart illustrating the method for generating an authenticated audio, image and/or video signal in accordance with the second embodiment is depicted in Fig. 2. Processing commences in step 200. In step 202, a check is made to determine if the operator is authorised, and if so authentication data is generated. In step 204, image, video, and/or audio data is captured if the operator is authorised. Steps 202 and 204 may be performed substantially simultaneously without departing from the scope and spirit of the invention. In step 206, the captured audio, image and/or video signal is watermarked with the authentication data. For further details of specific steps to be carried out, reference is made to the functionality of the apparatus of the first embodiment described above with reference to Fig. 1.

An apparatus in accordance with a third embodiment of the invention is depicted in Fig. 3. Features of the first embodiment that have corresponding parts in the third embodiment are denoted with a corresponding reference numeral. Thus, the authentication module 102 of Fig. 1 is denoted with reference numeral 302 in Fig. 3. For the purpose of brevity in the description, reference is simply made to the description of those corresponding modules in the description hereinbefore and not repeated here. Only the new elements of Fig. 3 are described in detail hereinafter. While the third embodiment illustrates two additional modules 318 and 320, it will be appreciated by one skilled in the art that the embodiment can be practiced optionally with only one of the two modules.

The recording device 300 includes a global positioning system (GPS) module 320 that can obtain accurate positioning information about the location of the recording device 324 when in operation. The GPS data 324 may be obtained at a predetermined instance or interval to be embedded in the captured signal 314 by the watermarking module 306. For example, after the operator is authenticated as authorised to operate the recording device 300 and when the capture module 304 is actuated, the GPS module 320 may obtain fresh GPS data or retrieve most recently stored GPS data to be provided as output 324 to the watermarking module 306.

Further, the recording device 300 can include an annotation module 318. The annotation module annotation module 318 can add annotation text, voice, or links to other media-segments directly into the media signal produced by the capture module 304 in a conventional manner. The annotation can be persistent and/or non-persistent. For example, a microphone and/or text input device can be included in the recording device 300 as part of the annotation module 318 for annotation purpose. Annotation information can be stored together with the media data based on a standard data format. For example, in the case of video media, the MPEG2 standard can be used which provides space for annotation. This is non-persistent annotation. Alternatively or in addition to non-persistent annotation, persistent annotation can be incorporated into the captured media signal 314.

The annotation module 318 also provides annotation signal 322 to the watermarking module 306. To make the annotation persistent, watermarking is used again to embed the annotation information 322 into the media data 314. Such persistent annotation can be either perceivable or non-perceivable. For example, persistent annotation is useful to put particular information at a particular location of an image. Alternatively, it can be used to put information in a particular interval of audio for indication of information like "this is John" or "sang by Linda". Therefore, the persistent and non-persistent annotation is useful to specify messages to be embedded in a captured media

signal, as well as information such as the location or time period which can be embedded in the media signal.

The foregoing embodiments of the invention disclose a method, apparatus and computer program product for generating an authenticated audio, image and/or video signal, where the authenticated signal is an audio, image and/or video signal watermarked with authentication data. The embodiments of the invention are advantageous in that they ameliorate or overcome one or more disadvantages of conventional audio, image and video capture systems. In particular, the embodiments of the invention are able to do so by requiring authentication data derived from an operator to operate a recording device and providing on-the-fly copyright ownership indicia in a recording by watermarking the recording using the authentication data. This is done in the recording device that is used to capture the audio, image and/or video work.

A small number of embodiments have been disclosed by way of example. However, those skilled in the art will recognise that the invention can be practiced, with modification, in the light of the information contained herein without departing from the scope and spirit of the invention.

The claims defining the invention are as follows:

1. A method of generating an authenticated audio, image and/or video signal, including:

generating an authentication signal;

capturing a digital audio, image and/or video signal; and

watermarking said digital audio, image and/or video signal using said authentication signal to provide said authenticated audio, image and/or video signal.

2. The method according to claim 1, wherein said step of generating said authentication signal is performed substantially simultaneously with said step of capturing said digital audio, image and/or video signal.

3. The method according to claim 1 or 2, wherein said authentication signal is derived from biometrics data, a password, user identification data, positioning data, chronological data, data transmitted from an external, remote source and/or data from a removable media.

4. The method according to any one of claims 1 to 3, wherein said step of capturing said digital audio, image and/or video signal includes:

capturing an analog audio, image and/or video signal; and

converting said analog audio, image and/or video signal to said digital audio, image and/or signal.

5. The method according to any one of claims 1 to 4, wherein said watermarking step provides perceptible and/or non-perceptible watermarks.

6. The method according to any one of claims 1 to 5, further including the step of annotating said digital audio, image and/or video signal using text and/or audio data.

7. The method according to any one of claims 1 to 6, wherein said annotating step is persistent and/or non-persistent.

8. The method according to any one of claims 1 to 7, further including the steps of:

determining if an operator is authorised to generate said authenticated audio, image and/or video signal; and

if so, enabling capture of said digital audio, image and/or video signal.

9. An apparatus for generating an authenticated audio, image and/or video signal, including:

means for generating an authentication signal;

means for capturing a digital audio, image and/or video signal; and

means for watermarking said digital audio, image and/or video signal using said authentication signal to provide said authenticated audio, image and/or video signal.

10. The apparatus according to claim 9, wherein said means for generating said authentication signal operates substantially simultaneously with said means for capturing said digital audio, image and/or video signal.

11. The apparatus according to claim 9 or 10, wherein said authentication signal is derived from biometrics data, a password, user identification data, positioning data, chronological data, data transmitted from an external, remote source and/or data from a removable media.

12. The apparatus according to any one of claims 9 to 11, wherein said means for capturing said digital audio, image and/or video signal includes:

means for capturing an analog audio, image and/or video signal; and

means for converting said analog audio, image and/or video signal to said digital audio, image and/or signal.

13. The apparatus according to any one of claims 9 to 12, wherein said means for watermarking provides perceptible and/or non-perceptible watermarks.

14. The apparatus according to any one of claims 9 to 13, further including means for annotating said digital audio, image and/or video signal using text and/or audio data.

15. The apparatus according to any one of claims 9 to 14, wherein said means for annotating provides persistent and/or non-persistent annotation.

16. The apparatus according to any one of claims 9 to 15, further including:

means for determining if an operator is authorised to generate said authenticated audio, image and/or video signal; and

means for enabling capture of said digital audio, image and/or video signal in response to determining said operator is authorised.

17. A computer program product having a computer readable medium having a computer program recorded therein for generating an authenticated audio, image and/or video signal, said computer program product including:

means for generating an authentication signal;

means for capturing a digital audio, image and/or video signal; and

means for watermarking said digital audio, image and/or video signal using said authentication signal to provide said authenticated audio, image and/or video signal.

18. The computer program product according to claim 17, wherein said means for generating said authentication signal operates substantially simultaneously with said means for capturing said digital audio, image and/or video signal.

19. The computer program product according to claim 17 or 18, wherein said authentication signal is derived from biometrics data, a password, user identification

data, positioning data, chronological data, data transmitted from an external, remote source and/or data from a removable media.

20. The computer program product according to any one of claims 17 to 19, wherein said means for capturing said digital audio, image and/or video signal includes:

means for capturing an analog audio, image and/or video signal; and

means for converting said analog audio, image and/or video signal to said digital audio, image and/or signal.

21. The computer program product according to any one of claims 17 to 20, wherein said means for watermarking provides perceptible and/or non-perceptible watermarks.

22. The computer program product according to any one of claims 17 to 21, further including means for annotating said digital audio, image and/or video signal using text and/or audio data.

23. The computer program product according to any one of claims 17 to 22, wherein said means for annotating provides persistent and/or non-persistent annotation.

24. The computer program product according to any one of claims 17 to 23, further including:

means for determining if an operator is authorised to generate said authenticated audio, image and/or video signal; and

means for enabling capture of said digital audio, image and/or video signal in response to determining said operator is authorised.

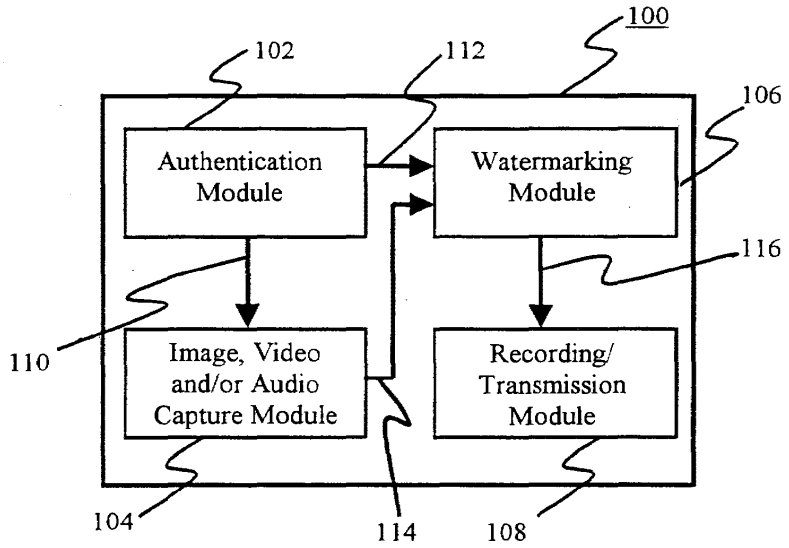

100
102
112
106
Authentication Module
Watermarking Module
116
110
Image, Video and/or Audio Capture Module
Recording/ Transmission Module
104
114
108

FIG. 1

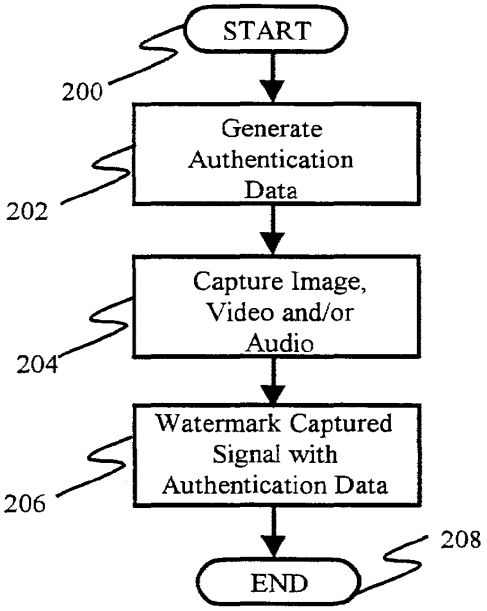

START
200
Generate Authentication Data
202
Capture Image, Video and/or Audio
204
Watermark Captured Signal with Authentication Data
206
208
END

FIG. 2

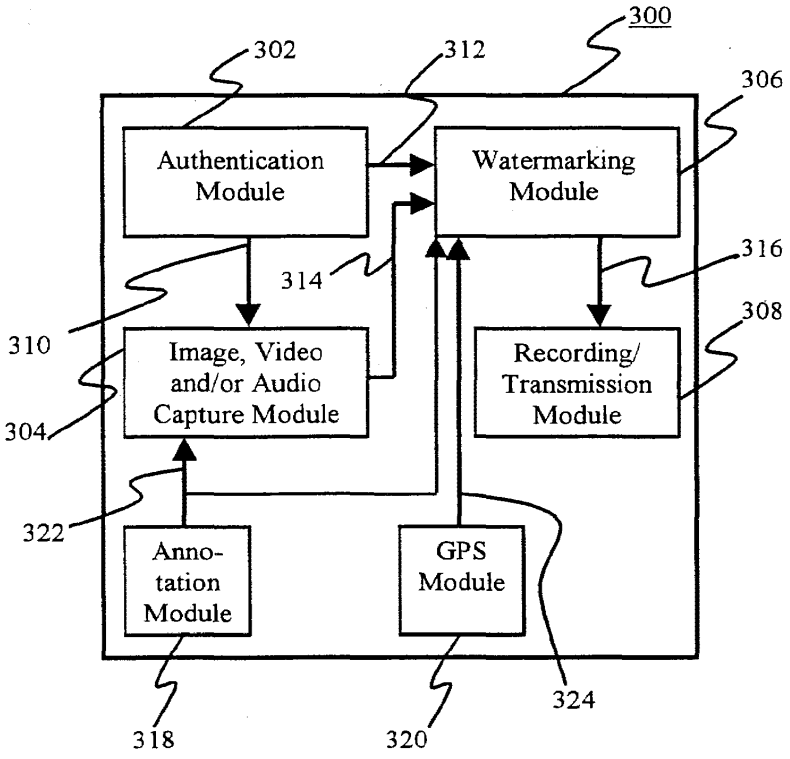

300
302
312
306
Authentication Module
Watermarking Module
314
316
310
308
Image, Video and/or Audio Capture Module
Recording/ Transmission Module
304
322
Anno-tation Module
GPS Module
324
318
320

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG 98/00104

A. CLASSIFICATION OF SUBJECT MATTER

IPC[6]: G 11 B 23/28, 23/36, 23/40

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)

IPC[6]: G 11 B 23/00; H 04 N 5/00, 7/00; G 07 C 9/00; H 04 L 9/00

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)

WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96/03 835 A2 (MACROVISION CORP.), 08 February 1996 (08.02.96), fig.1-3; abstract; claim 1.	1-5,9-12
A	EP 0 779 602 A2 (AT & T CORP.), 18 June 1997 (18.06.97), fig.1,4; abstract; claim 1.	1-16
A	US 5 598 473 A (LINSKER et al.), 28 January 1997 (28.01.97), abstract; fig.1,2; claim 1.	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„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)
„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

„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
„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
„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
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 January 1999 (25.01.99)	01 September 1999 (01.09.99)

Name and mailing adress of the ISA/AT	Authorized officer
Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna Facsimile No. 1/53424/200	Berger Telephone No. 1/53424/453

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG 98/00104

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [X] Claims Nos.: 17 to 24
because they relate to subject matter not required to be searched by this Authority, namely:
the features of these claims 17 to 24 disclose a computer program.

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:

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.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SG 98/00104

Im Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
WO A2 9603835	08-02-96	AU A1 31276/95	22-02-96
		AU B2 697727	15-10-98
		BR A 9508340	09-09-97
		CA AA 2195939	08-02-96
		CN A 1159272	10-09-97
		EP A2 775418	28-05-97
		JP T2 10503338	24-03-98
		NZ A 290521	28-10-98
		US A 5574787	12-11-96
		WO A3 9603835	04-04-96
EP A2 779602	18-06-97	CA AA 2188975	16-06-97
		JP A2 9179583	11-07-97
		US A 5761329	02-06-98
US A 5598473	28-01-97	US A 5680455	21-10-97

Form PCT/ISA/210 (patent family annex) (July 1998)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification [7] :
G09C 5/00, G06F 17/00, G06K 7/00, 9/00, 9/36, 19/06, H04L 9/00

A1

(11) International Publication Number: **WO 00/70585**

(43) International Publication Date: 23 November 2000 (23.11.00)

(21) International Application Number: PCT/US00/13333

(22) International Filing Date: 15 May 2000 (15.05.00)

(30) Priority Data:

09/314,648	19 May 1999 (19.05.99)	US
09/342,688	29 June 1999 (29.06.99)	US
09/342,689	29 June 1999 (29.06.99)	US
09/342,971	29 June 1999 (29.06.99)	US
09/343,101	29 June 1999 (29.06.99)	US
09/343,104	29 June 1999 (29.06.99)	US
60/141,468	29 June 1999 (29.06.99)	US
60/151,586	30 August 1999 (30.08.99)	US
60/158,015	6 October 1999 (06.10.99)	US
60/163,332	3 November 1999 (03.11.99)	US
60/164,619	10 November 1999 (10.11.99)	US
09/531,076	18 March 2000 (18.03.00)	US
09/543,125	5 April 2000 (05.04.00)	US
09/547,664	12 April 2000 (12.04.00)	US
09/552,998	19 April 2000 (19.04.00)	US

(71) Applicant *(for all designated States except US)*: DIGIMARC CORPORATION [US/US]; Suite 250, 19801 SW 72nd Avenue, Tualatin, OR 97062 (US).

(72) Inventors; and

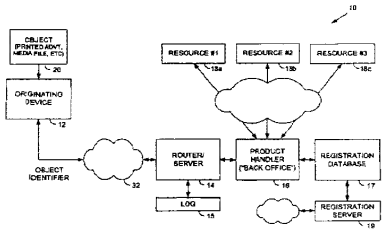
(75) Inventors/Applicants *(for US only)*: RHOADS, Geoffrey, B. [–/US]; 304 SW Tualatin Loop, West Linn, OR 97068 (US). RODRIGUEZ, Tony, F. [–/US]; 3104 NE 31st Avenue, Portland, OR 97212 (US). DAVIS, Bruce, L. [–/US]; 15599 Village Drive, Lake Oswego, OR 97034 (US). CARR, J., Scott [–/US]; 7814 SW 189th Avenue, Beaverton, OR 97007 (US). GROSSI, Brian, J. [–/US]; 220 Sleeper Avenue, Mountain View, CA 94040 (US). MCKINLEY, Tyler, J. [–/US]; 17020 SW Tracy Avenue, Lake Oswego, OR 97035 (US). SEDER, Phillip, A. [–/US]; 1600 Palatine Street, Portland, OR 97219 (US). PERRY, Burt, W. [–/US]; 15344 Provincial Hill Way, Lake Oswego, OR 97035 (US). HEIN, William, C., III [–/US]; 151 Indiantown Road, Glenmoore, PA 19343–1412 (US). MACINTOSH, Brian, T. [–/US]; 1200 Fairway Road, Lake Oswego, OR 97034 (US).

(74) Agent: CONWELL, William, Y.; Digimarc Corporation, 19801 SW 72nd Avenue, Suite 250, Tualatin, OR 97062 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, 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), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, 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: METHODS AND SYSTEMS FOR CONTROLLING COMPUTERS OR LINKING TO INTERNET RESOURCES FROM PHYSICAL AND ELECTRONIC OBJECTS



(57) Abstract

Physical or electronic objects are encoded with identifiers, which serve to trigger object–appropriate responses from computer systems that encounter such objects. The encoding may be steganographic (e.g., by digital watermarks), so the presence of such identifiers is not evident to persons encountering the objects. An exemplary application is a computer system that looks at a printed magazine advertisement (20) and initiates a link to a corresponding internet page. In one such implementation, the computer system senses an identifer encoded in the advertisement, forwards the identifier to a remote database, receives from the database (17) a corresponding internet address (18a, 18b, 18c), and directs a browser to that address (18a, 18b, 18c). The same arrangement can be used for on–line ordering from printed merchandise catalogs. Another application is a computer system that looks at a printed spreadsheet (20), and retrieves from disk storage an electonic version of the same document for editing.

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		

METHODS AND SYSTEMS FOR CONTROLLING COMPUTERS OR LINKING TO INTERNET RESOURCES FROM PHYSICAL AND ELECTRONIC OBJECTS

Background and Summary of the Invention

"Bedoop." That might be the sound someone might hear as they lazily place a magazine advertisement in front of their desktop camera. Magically, the marketing and sales web site associated with the ad is displayed on their computer. More information? Want to buy now? Look at the full product line? No problem.

"Bedoop." That might be the same sound when that same someone places their credit card in front of their desktop camera. Instantly, the product displayed on the web page is purchased. Behind the scenes, a secure purchase link is initiated, transmitting all requisite information to the vendor. Twist the credit card clockwise and the purchaser chooses overnight delivery.

So goes an exemplary embodiment further described in this specification. Although this example is rather specific, it nevertheless alludes to vast array of applications possible when an input device such as a digital camera is turned into a general-purpose user interface device with an intuitive power that very well might rival the mouse and the keyboard.

One aspect of certain embodiments is that an object or paper product so-scanned contains digital information that can be quickly read and acted upon by an appropriately configured device, computer or appliance. Such an embodiment envisions that this digital information is aesthetically hidden on objects. These objects have been previously and pro-actively marked with the digital information, using any of the broad range of data encoding technologies, such as digital watermarking.

Although this aspect of the technology concentrates on flat object applications wherein the digital information is often imperceptibly integrated into the object, it is certainly not meant to be so limited. Objects can be three dimensional in nature and the information more visually overt and/or pre-existing (i.e., not "pro-actively" embedded, or it might not even be "digital," per se). Different implementation considerations attach to these variants. Likewise, though the bulk of this disclosure concentrates on objects which have some form of digital message attached thereto, some aspects of the technology may apply to objects which have no such thing, where the prior arts of pattern recognition and gestural input can be borrowed in combination with this technology to effect yet a broader array of applications.

Nor, as will be apparent, is the technology limited to systems employing optical input and encoded imagery. Corresponding techniques can also be employed with encoded audio. Indeed, any physical or electronic "object" can make use of the principles detailed herein.

"Bedoop." The sound that a refrigerator might make, outfitted with a simple camera/ processor unit/net connection, as a ten year old child holds up an empty milk carton and a ping goes out to the local grocery store, adding the item to an accumulating delivery list. The sound that might be heard echoing over and over inside Internet cafés as heretofore computerphobes take their first skeptical steps onto the World Wide Web. The sound heard at the fast food counter as a repeat customer holds up his sandwich

card ticking off his latest meal, hoping for the sirens to go off for a $500 prize given to the lucky customer of the week. Blue sky scenarios abound.

Such aspects of the present technology are thus about powerful new user interfaces to computers. These new user interfaces extend into the everyday world in ways that a mouse and keyboard never could. By enabling everyday objects to communicate their identities and functions to ever-attendant devices, not only will the World Wide Web be given an entirely new dimension, but basic home and office computing may be in store for some fundamental advances as well.

According to one aspect, the invention includes a method of data processing on a computer system, comprising (a) using an application program to compose an electronic version of a document; (b) printing the document onto paper, the printing including marking with machine readable indicia encoding plural-bit auxiliary data; and (c) storing the plural-bit auxiliary data in association with data identifying a location at which the electronic version of the document is stored.

According to another aspect, the invention includes a method of data processing on a computer system, comprising (a) presenting a printed document to an optical capture device; (b) processing image data produced by said device to decode plural-bit data encoded therein; (c) based on said decoded plural-bit data, launching a software application corresponding to said printed document; and (d) using said software application to open an electronic version of said document.

According to another aspect, the invention includes a method of operating a computer, the computer including an operating system with a registry database, the registry database associating specific data types with specific software programs particularly corresponding thereto, wherein the method further includes: (a) providing a frame of image data; (b) decoding plural-bit identifier data from the image data; (c) consulting the registry database to identify a software program corresponding to said identifier data; and (d) invoking the identified software program.

According to another aspect, the invention includes a greeting card having a substrate with visually-perceptible indicia printed thereon, wherein the card is encoded with plural-bit binary data that can be decoded by an image processing device and used to direct a computer to a web site where an image, video, and/or audio presentation corresponding to said card is provided.

According to another aspect, the invention includes a method of providing a customized greeting, comprising: (a) providing a greeting card having plural-bit data encoded therein; (b) customizing a web site presentation corresponding to said card; (c) providing the card to a recipient; (d) decoding the encoded plural-bit data from the card; and (e) in response to the decoded plural-bit data, presenting to the recipient the web site presentation.

According to another aspect, the invention includes a method of printing a magazine, comprising: (a) processing an electronic representation of an advertisement to encode plural bit data therein; (b) printing a page of advertising in accordance with said electronic representation to yield an encoded advertisement page; and (c) binding said page into a magazine; wherein said plural bit data serves to identify an entry in a database, said database entry having an internet address of a web page that is associated with said advertisement stored therein.

According to another aspect, the invention includes a promotional method comprising: (a) encoding a print advertisement to hide plural-bit data therein; (b) processing the print advertisement to extract the plural-bit data therefrom; and (c) using at least a part of the extracted plural-bit data to direct an internet web browser to a web site that provides consumer information related to a product or service promoted by the print advertisement.

According to another aspect, the invention includes a method of determining consumer response to print advertising, comprising: (a) encoding a first print advertisement with first data; (b) encoding a second print advertisement with second data different than the first; (c) the first and second data providing identifiers by which consumer devices can link to web pages associated with said advertisements; (d) monitoring linking traffic due to each of said identifiers to thereby determine consumer response to the advertisements.

According to another aspect, the invention includes a promotional method comprising: (a) presenting an object within the field of view of an optical sensor device, the object being selected from the list consisting of a retail product, packaging for a retail product, or printed advertising; (b) acquiring optical data corresponding to the object; (c) decoding plural-bit digital data from the optical data; (d) submitting at least some of said decoded data to a remote computer; and (e) determining at the remote computer whether a prize should be awarded in response to submission of said decoded data.

According to another aspect, the invention includes a method of interacting with a magazine using a computer, the computer including an internet web browser, the method including: (a) providing a peripheral device having a sensor; (b) positioning the peripheral device adjacent a first advertisement in the magazine to direct the web browser to a first internet address; and (c) positioning the peripheral device adjacent a second advertisement in the magazine to direct the web browser to a second internet address.

According to another aspect, the invention includes a computer peripheral and method of its use, the peripheral being used in conjunction with a computer system having an internet browser associated therewith, the peripheral comprising: (a) a housing adapted to fit within a user's palm and slide over a medium; (b) an optical sensor having at least one sensing element and producing optical data; (c) a lens for imaging the medium onto the sensor; and the method includes: (a) sliding the peripheral over a portion of a printed advertisement; (b) processing the optical data to decode plural bit information encoded on the advertisement; and (c) using said plural bit information to direct the internet browser to an internet web page associated with said advertisement.

According to another aspect, the invention includes an electronic commerce method comprising: (a) providing a printed catalog that includes an image of an article offered for sale by a merchant, wherein the image is encoded with plural-bit binary data; (b) optically sensing the image to produce optical data corresponding thereto; (c) decoding the encoded data from the optical data; and (d) electronically ordering the article from the merchant by use of said decoded data. The ordering may make use of earlier-stored customer profile information (e.g., clothing size data), and the encoding may be steganographic.

According to another aspect, the invention comprises a wireless telephony handset including a microphone, a modulator, and an RF amplifier, the device serving to receive audio and transmit an RF signal conveying audio modulation, the handset further including an optical sensor producing optical data, a lens for imaging an object onto the sensor, and a decoder for decoding plural bit identifier data conveyed by a barcode or a digital watermark on the object.

According to another aspect, the invention includes an image-based network navigation method permitting a user to link to a remote computer, comprising: (a) detecting encoded data from a printed object; (b) linking to the remote computer through a network in accordance with said encoded data; and (c) providing the user's zip code to the remote computer.

According to another aspect, the invention includes a method comprising: (a) sensing an object identifier from a first object; (b) sending said first object identifier from a first device to a second device; (c) in response, at said second device, identifying address information corresponding to said first object identifier and sending same to the first device; (d) initiating a link from the first device in accordance with said address information; (e) at said second device, identifying additional objects related to said first object; identifying additional address information corresponding to said additional objects; and sending said additional address information to the first device; and (f) storing said additional address information in a memory at the first device; wherein, if an object included among said identified additional objects is sensed by the first device, the corresponding address information can be retrieved from said memory in the first device without the intervening delays of communicating with the second device.

According to another aspect, the invention includes an apparatus having a detector of machine readable data and a software program used in conjunction with said machine readable data, operable to transmit a packet of data to a remote system, said packet of data comprising (a) an identifier of said software program, and (b) at least a portion of detected machine readable data.

According to another aspect, the invention includes an apparatus having a detector of machine readable data and a software program used in conjunction with said machine readable data, operable to transmit a packet of data to a remote system, said packet of data comprising (a) a context or environment identifier, and (b) at least a portion of detected machine readable data.

According to another aspect, the invention includes a networked computer system, responsive to watermark data sent from a software program on a remote computer, to initiate delivery of advertisement data to said remote computer.

In any of the foregoing arrangements, the encoding can be steganographic (e.g., by digital watermarking), or can employ other machine readable data (e.g., barcodes, etc.). More generally, the arrangements just reviewed generally have counterparts that can be implemented with other than optical or image data (e.g., audio data, magnetic stripe information, etc.).

The foregoing just touches on a few of the many inventive aspects of the technology detailed below. These and other features of the present technology will be more readily apparent from the following detailed description, which proceeds with reference to the accompanying drawings.

Brief Description of the Drawings

Fig. 1 is a diagram showing the principal process components of an illustrative system employing the present technology.

Fig. 2 is a block diagram showing an illustrative system for performing the response process of Fig. 1.

Fig. 3 is a block diagram more particularly detailing an originating device used in the system of Fig. 2.

Fig. 4 illustrates certain top level data flows in the system of Fig. 2.

Fig. 5 illustrates certain data flows associated with the router of Fig. 2.

Fig. 6 illustrates certain data flows associated with the registration process of Fig. 2.

Fig. 7 illustrates certain data flows associated with the product handler of Fig. 2.

Figs. 8-10 show a sequence of screen shots from an illustrative system.

Fig. 11 is a block diagram showing another embodiment of the present technology.

Fig. 12 is a block diagram showing another embodiment of the present technology.

Fig. 13 is a block diagram of a prior art scanner.

Fig. 14 shows an object being scanned along an arced path.

Fig. 15 shows how object warping may be detected.

Fig. 16 shows use of binocular processing to determine certain object attributes.

Fig. 17 shows a watermark grid.

Fig. 18 shows a pre-warped watermark grid.

Fig. 19 shows another pre-warped watermark grid.

Detailed Description

Basically, the technology detailed in this disclosure may be regarded as enhanced systems by which users can interact with computer-based devices. Their simple nature, and adaptability for use with everyday objects (e.g., milk cartons), makes the disclosed technology well suited for countless applications.

Due to the great range and variety of subject matter detailed in this disclosure, an orderly presentation is difficult to achieve. For want of a better arrangement, the specification is broken into two main parts. The first part details a variety of methods, applications, and systems, to illustrate the diversity of the present technology. The second more particularly focuses on a print-to-internet application. A short concluding portion is presented in Part III.

As will be evident, many of the topical sections presented below are both founded on, and foundational to, other sections. For want of a better rationale, the sections in the first part are presented in a more or less random order. It should be recognized that both the general principles and the particular details from each section find application in other sections as well.

Compounding the situation, the present specification draws from several priority applications filed over the course of nearly a year. Accordingly, the same concepts are sometimes expressed several

times, each reflecting a different perspective – depending on the date and context of the application in which it was first found.

The term "Bedoop" has been superceded in applicant's commercialization of the technology by the term Digimarc MediaBridge. Both terms are used in this specification but refer to the same technology.

To prevent the length of this disclosure from compounding out of control, the various permutations and combinations of the features of the different sections are not exhaustively detailed. The inventors intend to explicitly teach such combinations/permutations, but practicality requires that the detailed synthesis be left to those who ultimately implement systems in accordance with such teachings.

PART I

Introduction to Digital Watermarking and other Encoding Techniques

There are nearly as many techniques for digital watermarking (a type of steganographic data encoding) as there are applications for it. The reader is presumed to be familiar with the great variety of methods. A few are reviewed below.

The present assignee's prior application 09/127,502, filed July 31, 1998, now published as WO0007356, shows techniques by which very fine lines can be printed on a medium to slightly change the medium's apparent tint, while also conveying digital data. Commonly-owned application 09/074,034, filed May 6, 1998, now published as WO 9953428, details how the contours of printed imagery can be adjusted to convey digital data. (That technique can be applied to printed text characters, as well as the line art imagery particularly considered.) The assignee's patent 5,850,481 details how the surface of paper or other media can be textured to convey optically-detectable binary data. The assignee's patents 5,862,260, 5,841,886 and 5,809,160 detail various techniques for steganographically encoding photographs and other imagery.

Some watermarking techniques are based on changes made in the spatial domain; others are based on changes made in transformed domains (e.g., DCT, wavelet).

Watermarking of printed text can be achieved by slight variations to character shape, character kerning, line spacing, etc., as shown by various writings by Brassil et al, including "Electronic Marking and Identification Techniques to Discourage Document Copying," Proceedings of INFOCOM '94 Conference on Computer, IEEE Comm. Soc Conference, June 12-16, 1994, pp. 1278-1287; "Hiding Information in Document Images," Proceedings of the Twenty-Ninth Annual Conference on Information Sciences and Systems, p. 482-9, 1995; and "Document marking and identification using both line and word shifting," Proceedings of IEEE INFOCOM '95, The Conference on Computer Communications. Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies; Bringing Information to People (Cat. No.95CH35759), p. 853-60 vol.2, 1995.

The foregoing is just a sampling of the large literature on watermarking. The artisan is presumed to be familiar with such art, all of which is generally suitable for use with the novel concepts detailed below.

Although the following specification focuses on applications employing digital watermarking, certain of such applications can alternatively employ other data encoding techniques, including 1D and 2D barcodes, magnetic ink character recognition (MICR), optical character recognition (OCR), optical mark recognition (OMR), radio frequency identification (RF/ID), UV/IR identification technologies, data glyphs, organic transistors, magnetic stripe, etc., depending on the particular application requirements.

Basic Principles – Refrigerators and Desktop Clutter

Referring to Fig. 11, a basic embodiment 110 of the present technology includes an optical sensor 112, a computer 114, and a network connection 116 to the internet 118. The illustrated optical sensor 112 is a digital camera having a resolution of 320 by 200 pixels (color or black and white) that stares out, grabbing frames of image data five times per second and storing same in one or more frame buffers. These frames of image data are analyzed by a computer 114 for the presence of Bedoop data. (Essentially, Bedoop data is any form of plural-bit data encoding recognized by the system 110 -- data which, in many embodiments, initiates some action.) Once detected, the system responds in accordance with the detected Bedoop data (e.g., by initiating some local action, or by communication with a remote computer, such as over the internet, via an online service such as AOL, or using point-to-point dial-up communications, as with a bulletin board system).

Consider the milk carton example. The artwork on a milk carton can be adapted to convey Bedoop data. In the preferred embodiment, the Bedoop data is steganographically encoded (e.g., digitally watermarked) on the carton. Numerous digital watermarking techniques are known – all of which convey data in a hidden form (i.e., on human inspection, it is not apparent that digitally encoded data is present). Exemplary techniques operate by slightly changing the luminance, or contours of selected points on artwork or text printed on the carton, or by splattering tiny droplets of ink on the carton in a seemingly random pattern. Each of these techniques has the effect of changing the local luminance at areas across the carton – luminance changes that can be detected by the computer 114 and decoded to extract the encoded digital data. In the case of a milk carton, the data may serve to identify the object as, e.g., a half gallon carton of Alpenrose brand skim milk.

The Fig. 11 apparatus can be integrated into the door of a refrigerator and used to compile a shopping list. Milk cartons, and other Bedoop-encoded packaging, can be held up the optical sensor. When the computer 114 detects the presence of Bedoop data and successfully decodes same, it issues a confirmation tone ("be-doop") from a speaker or other audio transducer 122. The computer then adds data identifying the just-detected object to a grocery list. This list can be maintained locally (in disk storage or non-volatile RAM 124 or the like in the refrigerator or elsewhere in the home), or remotely (e.g., at a server computer located at a user-selected grocery, or elsewhere). In either event, the list is desirably displayed on a display in the user's home (e.g., an LCD screen 126 built into the front of the appliance). Conventional user interface techniques can be employed permitting the user to scroll through the displayed list, delete items as desired, etc.

Periodically, the listed groceries can be purchased and the list cleared. In one embodiment, the list is printed (either at the home or at the grocery), and the user walks the grocery aisles and purchases same in the conventional manner. In another embodiment, the grocer pulls the listed items from the shelves (in response to a user request conveyed by the internet or telephone, or by a gesture as hereafter detailed). Once the list has been pulled, the grocer can alert the user that the groceries are available for pickup (again, e.g., by internet or telephone message), or the grocer can simply deliver the groceries directly to the user's home. Naturally, on-line payment mechanisms can be employed if desired.

Consider a wholly unrelated Bedoop application. A Microsoft Excel spreadsheet is printed onto paper, and the paper becomes buried in a stack of clutter on an office worker's desk. Months later the spreadsheet again becomes relevant and is dug out of the stack. Changes need to be made to the data, but the file name has long-since been forgotten. The worker simply holds the printed page in front of a camera associated with the desktop computer. A moment later, the electronic version of the file appears on the worker's computer display.

When the page was originally printed, tiny droplets of ink or toner were distributed across the paper in a pattern so light as to be essentially un-noticeable, but which steganographically encoded the page with a plural-bit binary number (e.g., 24-128 bits). A database (e.g., maintained by the operating system, the Excel program, the printer driver, etc.) stored part of this number (e.g., 20 bits, termed a Universal Identifier, or UID) in association with the path and file name at which the electronic version of the file was stored, the page number within the document, and other useful information (e.g., author of the file, creation date, etc.).

The steganographic encoding of the document, and the updating of the database, can be performed by the software application (e.g., Excel). This option can be selected once by the user and applied thereafter to all printed documents (e.g., by a user selection on an "Options" drop-down menu), or can be presented to the user as part of the Print dialog window and selected (or not) for each print job.

When such a printed page is later presented to the camera, the computer automatically detects the presence of the encoded data on the page, decodes same, consults the database to identify the file name/location/page corresponding to the 20-bit UID data, and opens the identified file to the correct page (e.g., after launching Excel). This application is one of many "paper as portal" applications of the Bedoop technology.

The foregoing are but two of myriad applications of the technology detailed herein. In the following discussion a great many other applications are disclosed. However, regardless of the length of the specification, it is possible only to begin to explore a few of the vast ramifications of this technology.

A few more details on the basic embodiments described above may be helpful before delving into other applications.

Optics

For any system to decode steganographically encoded data from an object, the image of the object must be adequately focused on the digital camera's CCD (or other, e.g., CMOS) sensor. In a low

cost embodiment, the camera has a fixed nominal focal length, e.g., in the range of 2-24 inches (greater or lesser lengths can of course be used). Since the camera is continuously grabbing and analyzing frames of data, the user can move the object towards- or away- from the sensor until the decoder succeeds in decoding the steganographically encoded data and issues a confirming "Bedoop" audio signal.

In more elaborate embodiments, known auto-focusing technology can be employed.

In still other embodiments, the camera (or other sensor) can be equipped with one or more auxiliary fixed-focus lenses that can be selectively used, depending on the particular application. Some such embodiments have a first fixed focused lens that always overlies the sensor, with which one or more auxiliary lenses can be optically cascaded (e.g., by hinge or slide arrangements). Such arrangements are desirable, e.g., when a camera is not a dedicated Bedoop sensor but also performs other imaging tasks. When the camera is to be used for Bedoop, the auxiliary lens is positioned (e.g., flipped into) place, changing the focal length of the first lens (which may by unsuitably long for Bedoop purposes, such as infinity) to an appropriate Bedoop imaging range (such as one foot).

Other lens-switching embodiments do not employ a fixed lens that always overlies the sensor, but instead employ two or more lenses that can be moved into place over the sensor. By selecting different lenses, focal lengths such as infinity, six feet, and one foot can be selected.

In all such arrangements, it is desirable (but not essential) that the steganographically-encoded portion of the object being imaged fills a substantial part of the image frame. The object can be of various sizes, e.g., a 10 by 12 inch front panel of a cereal box, or a proof of purchase certificate that is just one inch square. To meet this requirement, small objects need to be placed closer to the camera than large objects. The optics of the system can be designed, e.g., by selection of suitable aperture sizing and auxiliary lighting (if needed), to properly image objects of various sizes within a range of focal distances.

Some embodiments avoid issues of focal distances and identifying the intended object by constraining the size of the object and/or its placement. An example is a business card reader that is designed for the sole task of imaging business cards. Various such devices are known.

Decoding/Encoding

The analysis of the image data can be accomplished in various known ways. Presently, most steganographic decoding relies on general purpose microprocessors that are programmed by suitable software instructions to perform the necessary analysis. Other arrangements, such as using dedicated hardware, reprogrammable gate arrays, or other techniques, can of course be used.

The steganographic decoding process may entail three steps. In the first, the object is located. In the second, the object's orientation is discerned. In the third, the Bedoop data is extracted from the image data corresponding to the Bedoop object.

The first step, object location, can be assisted by various clues. One is the placement of the object; typically the center of the image field will be a point on the object. The surrounding data can then be analyzed to try and discern the object's boundaries.

Another location technique is slight movement. Although the user will typically try to hold the object still, there will usually be some jitter of the Bedoop object within the image frame (e.g., a few pixels back and forth). Background visual clutter, in contrast, will typically be stationary. Such movement may thus be sensed and used to identify the Bedoop object from within the image data.

Still another object-location clue is object shape. Many Bedoop objects are rectangular in shape (or trapezoidal as viewed by the camera). Straight edge boundaries can thus be used to define an area of likely Bedoop data.

Color is a further object identification clue that may be useful in some contexts.

Yet another object location clue is spatial frequency. In imaging systems with well defined focal zones, undesired visual clutter may be at focal distances that results in blurring. The Bedoop object, in contrast, will be in focus and may be characterized by fine detail. Analyzing the image data for the high frequencies associated with fine detail can be used to distinguish the intended object from others.

Characteristic markings on the object (as discussed below in connection with determining object orientation) can also be sensed and used in locating the object.

Once the Bedoop object has been located within the image data, masking can be applied (if desired) to eliminate image data not corresponding to the intended object.

The next step in the decoding process, determining orientation of the Bedoop data, can likewise be discerned by reference to visual clues. For example, some objects include subliminal graticule data, or other calibration data, steganographically encoded with the Bedoop data to aid in determining orientation. Others can employ overt markings, either placed for that sole purpose (e.g. reference lines or fiducials), or serving another purpose as well (e.g. lines of text), to discern orientation. Edge-detection algorithms can also be employed to deduce the orientation of the object by reference to its edges.

Some embodiments filter the image data at some point in the process to aid in ultimate Bedoop data extraction. One use of such filtering is to mitigate image data artifacts due to the particular optical sensor. For example, CCD arrays have regularly-spaced sensors that sample the optical image at uniformly spaced discrete points. This discrete sampling effects a transformation of the image data, leading to certain image artifacts. An appropriately configured filter can reduce some of these artifacts.

(In some arrangements, the step of determining the orientation can be omitted. Business card readers, for example, produce data that is reliably free of artifacts and is of known scale. Or the encoding of the Bedoop data can be effected in such a way that renders it relatively immune to certain distortion mechanisms. For example, while the presently-preferred encoding arrangement operates on a 2D grid basis, with rows and columns of data points, the encoding can alternatively be done on another basis (e.g., a rotationally-symmetric form of encoding, so that rotational state of the image data can be ignored). In still other embodiments, the orientation-determining step can be omitted because the decoding can readily proceed without this information. For example decoding which relies on the Fourier-Mellin transform produces data in which scale and rotation can be ignored.)

Once the orientation of the object is discerned, the image data may be virtually re-registered, effectively mapping it to another perspective (e.g., onto a rectilinear image plane). This mapping can employ known image processing techniques to compensate, e.g., for rotation state, scale state, differential scale state, and X-Y offset, of the original Bedoop image data. The resulting frame of data may then be more readily processed to extract the steganographically-encoded Bedoop data.

In an exemplary embodiment, after the image data is remapped into rectilinear planar form, subliminal graticule data is sensed that identifies the locations within the image data where the binary data is encoded. Desirably, the binary data is redundantly encoded, e.g., in blocks of eight-by-eight patches. Each patch comprises one or more pixels. (The patches are typically square, and thus contain 1, 4, 9, or 16, etc. pixels.) The nominal luminance of each patch before encoding (e.g., artwork pre-existing on the object) is slightly increased or decreased to encode a binary "1" or "0." The change is slight enough to be generally imperceptible to human observers, yet statistically detectable from the image data – especially if several such blocks are available for analysis. Preferably, the degree of change is adapted to the character of the underlying image, with relatively greater changes being made in regions where the human eye is less likely to notice them. Each block thus encoded can convey plural bits of data (e.g., 16 – 128 bits). The encoding of such blocks in tiled fashion across the object permits the data to be conveyed in robust fashion.

Much of the time, of course, the Bedoop sensor is staring out and grabbing image frames that have no Bedoop data. Desirably, the detection process includes one or more checks to assure that Bedoop data is not wrongly discerned from non-Bedoop image data. Various techniques can be employed to validate the decoded data, e.g., error detecting codes can be included in the Bedoop payload and checked to confirm correspondence with the other Bedoop payload. Likewise, the system can confirm that the same Bedoop data is present in different tiled excerpts within the image data, etc.

Details of particular encoding and decoding techniques can be found in U.S. patent 5,862,260 and application 09/503,881. As noted, the data can be encoded on a tiled basis, with each tile being 64 to 256 elements on a side. Each element can be 0.01 inches square. The Bedoop payload data can be redundantly represented by various error-tolerant coding techniques (e.g., convolutions coding, trellis coding, turbo codes, etc.) to fill the tiled block. Each bit is thus redundantly encoded, with a "1" being represented as an increase at certain pixels, and as a decrease at other pixels. The increases and decreases can be scaled in accordance with visual masking attributes of the image being encoded. The calibration signal can be summed with the tiled data signal and can comprise a signal tailored in the frequency domain to have 12 – 64 spectral impulses per quadrant, in a known pattern. During detection, the rotation or scaling of these impulses from their known frequency domain coordinates permits the rotation or scaling of the image to be discerned and compensated for.

Data Structures, Formats, Protocols, and Infrastructures

In an exemplary system, the Bedoop data payload is 64 bits. This payload is divided into three fields CLASS (12 bits), DNS (24 bits) and UID (24 bits). (Other payload lengths, fields, and divisions, are of course possible, as is the provision of error-checking or error-correcting bits.)

Briefly, the CLASS ID is the most rudimentary division of Bedoop data, and may be analogized, in the familiar internet taxonomy, to the limited number of top level domains (e.g., .com, .net, .org, .mil, .edu, .jp, .de, .uk, etc.). It is basically an indicator of object type. The DNS ID is an intermediate level of data, and may be analogized to internet server addresses (e.g., biz.yahoo, interactive.wsj, etc.) The UID is the finest level of granularity, and can roughly be analogized to internet pages on a particular server (e.g., edition/current/summaries/front.htm, daily/home/default.hts, etc.).

Generally speaking, the CLASS ID and DNS ID, collectively, indicate to the system what sort of Bedoop data is on the object. In the case of Bedoop systems that rely on remote servers, the CLASS and DNS IDs are used in identifying the server computer that will respond to the Bedoop data. The UID determines precisely what response should be provided.

In the case of a refrigerator Bedoop system, what happens if an object with an unfamiliar CLASS/DNS ID data is encountered? The system can be programmed not to respond at all, or to respond with a raspberry-like sound (or other feedback) indicating, "I see a Bedoop object but don't know what to do with it."

Most systems will be able to respond to several classes of Bedoop objects. Simple software-based systems can compare the CLASS/DNS ID (and optionally the UID) to fixed values, and can branch program execution to corresponding subroutines. Likewise, hardware-based systems can activate different circuitry depending on the detected CLASS/DNS ID.

In the case of a computer equipped with a Bedoop input device (e.g., a Sony VAIO PictureBook laptop with built-in camera, or a desktop personal computer with a tethered camera), the operating system's registry database can be employed to associate different application programs with different CLASS/DNS IDs (just as the .XLS and .DOC file extensions are commonly associated by existing operating system registries to invoke Microsoft Excel and Word software applications, respectively). When a new Bedoop application is installed, it logs an entry in the registry database indicating the CLASS/DNS ID(s) that it will handle. Thereafter, when an object with such a CLASS/DNS ID is encountered, the operating system automatically launches the corresponding application to service the Bedoop data in an appropriate manner.

Sometimes the computer system may encounter a Bedoop object for which it does not have a registered application program. In such case, a default Bedoop application can be invoked. This default application can, e.g., establish an internet link to a remote server computer (or a network of such computers), and can transmit the Bedoop data (or a part of the Bedoop data) to that remote computer. The remote server can undertake the response itself, it can instruct the originating computer how to respond appropriately, or it can undertake some combination of these two responses. (Such arrangements are further considered below.)

Fig. 12 shows an illustrative architecture employing the foregoing arrangement.

At a local Bedoop system 128 (which may be implemented, for example, using a conventional personal computer 129), a camera, scanner, or other optical sensor 130 provides image data to a decoder 132 (which may be implemented as a software component of the operating system 133). The decoder 132 analyzes the image data to discern the plural-bit Bedoop data. The CLASS ID of this Bedoop data is applied to a Bedoop registry 134. The registry responds by identifying and launching a local Bedoop application 136 designed to service the discerned Bedoop data.

Sometimes the system 128 may encounter a Bedoop object for which several different responses may be appropriate. In the case of a printed office document, for example, one response may be as described above – to present the electronic version of the file on a computer, ready for editing. But other responses may also be desired, such as writing an email message to the author of the printed document, with the author's email address already specified in the message address field, etc.

Such different responses may be handled by different Bedoop applications, or may be options that are both provided by a single Bedoop application. In the former case, when the CLASS/DNS IDs are decoded and provided to the operating system, the registry indicates that there are two (or more) programs that might be invoked. The operating system can then present a dialog box to the user inviting the user to specify which form of response is desired. Optionally, a default choice can be made if the user doesn't specify within a brief period (e.g., three seconds). The operating system can then launch the Bedoop application corresponding to the chosen response.

A similar arrangement can be employed if a single Bedoop application can provide both responses. In such case the operating system launches the single Bedoop application (since there is no ambiguity to be resolved), and the application presents the choice to the user. Again, the user can select, or a default choice can be automatically made.

In the just-described situations, the user can effect the choice by using the keyboard or mouse – as with traditional dialog boxes. But Bedoop provides another, usually easier, form of interaction. The user can make the selection through the optical sensor input. For example, moving the object to the right can cause a UI button on the right side of the dialog box to be selected; moving the object to the left can cause a UI button on the left side of the dialog box to be selected; moving the object towards the camera can cause the selected button to be activated. Many other such techniques are possible, as discussed below.

If the registry 134 does not recognize, or otherwise does not know how to respond to Bedoop data of that particular CLASS/DNS, the registry launches a default Bedoop client application. This client application, in turn, directs a web browser 40 on the local Bedoop system 128 to communicate with a remote master registration server computer 42. The local computer forwards the Bedoop data to this master server. The master server 42 examines the CLASS ID, and forwards the Bedoop data (directly, or through intervening servers) to a corresponding CLASS server 44. (A single server may handle Bedoop data of several classes, but more typically there is a dedicated server for each CLASS.)

Each CLASS server 44 serves as the root of a tree 46 of distributed DNS servers. A DNS server 48a, for example, in a first tier 50 of the DNS server tree, may handle Bedoop data having DNS IDs beginning with "000." Likewise, DNS server 48b may handle Bedoop data having DNS IDs beginning with "001," etc., etc.

Each DNS server in the first tier 50 may, in turn, route Bedoop data to one of 8 servers in a second tier of the tree, in accordance with the fourth- through sixth bits of the DNS data. The tree continues in this fashion until a terminal level of DNS leaf node servers 56.

Ultimately, Bedoop data routed into this network reaches a DNS leaf node server 56. That leaf node server may handle the Bedoop data, or may redirect the local Bedoop system to a further server 58 that does so. That ultimate server – whether a DNS leaf node server or a further server – can query the local Bedoop system for further information, if necessary, and can either instruct the local Bedoop system how to respond, or can undertake some or all of the response itself and simply relay appropriate data back to the local Bedoop system.

In arrangements in which the local Bedoop system is redirected, by the DNS leaf node server, to a further server that actually handles the response, access to the further server may be through a port 59 (e.g., a special URL) tailored to receipt of Bedoop data.

In a typical implementation, most or all of the servers are mirrored, or otherwise replicated/redundant, so that failure of individual computers does not impair operation of the system.

Caching can be provided throughout the trees of servers to speed responses. That is, responses by leaf nodes for certainly commonly-encountered CLASS/DNS IDs can be temporarily stored earlier in the tree(s). Bedoop data, propagating through the server network, can prompt a response from an intermediate server if there is a cache hit.

If desired, Bedoop traffic through the above-detailed server trees can be monitored to collect demographic and statistical information as to what systems are sending what Bedoop data, etc. One use of such information is to dynamically reconfigure the DNS network to better balance server loads, to virtually relocate DNS resources nearer regions of heavy usage, etc. Another use of such information is for marketing purposes, e.g., to promote certain Bedoop features and applications within user groups (e.g., internet domains) that seem to under-utilize those features.

Within certain user networks that are linked to the internet, e.g., corporate networks, Bedoop data that isn't handled within the originating Bedoop system may first be routed to a Bedoop name server within the corporate network. That server will recognize certain types of Bedoop data, and know of resources within the corporate network suitable for handling same. Referral to such resources within the corporate network will be made, where possible. These resources (e.g., corporate servers) may respond to Bedoop data in a way customized to the corporate preferences. If the corporate Bedoop name server does not know of a resource within the corporate network that can respond to the Bedoop data, the corporate name server then routes the data to the public Bedoop network described above. (Such referral can be to the master registration server or, to the extent the corporate name server knows the addresses of

appropriate servers within the DNS server tree, or of the further servers to which DNS servers may point for certain Bedoop data, it can redirect the local Bedoop system accordingly.)

In typical rich Bedoop implementations, local systems may have libraries of Bedoop services, applications, or protocols. Some may be unique to that computer. Others may be commonly available on all computers. Some may be highly secure, employing encryption and/or anti-hacking measures, or data protocols that are not generally recognized. Others may be shareware, or the result of open-source programming efforts.

While the just-described arrangements used a 12/24/24 bit protocol for CLASS/DNS/UID data, other arrangements can of course be used. In some applications it is advantageous for the protocol to more nearly match those commonly used for internet communications. For example, IP addresses for internet Domain Name Servers (DNS) are presently 32 bits, with extension to 64 or 128 bits foreseen in the near future. The DNS field in Bedoop systems can be follow the internet standard.

Greeting Cards, Birthday Cards, Etc.

To further illustrate some of the basic principles associated with this technology, consider greeting cards and the like that are encoded (e.g., by texturing, printing, etc.) with Bedoop data. On receiving such a card, a recipient holds it in front of the image capture device on a laptop or other computer. The computer responds by displaying an internet web page that has a stock- or customized-presentation (image, video, audio-video, etc.) to complement that presented on the greeting card.

The web site presentation can be personalized by the sender (e.g., with a text message, recent family photographs, etc.), either at the point of card sale, or sometime after the card is purchased. In the latter case, for example, the card can be serialized. After taking the card home, the purchaser can visit the card vendor's web site and enter the card serial number in an appropriate user interface. The purchaser is then presented with a variety of simple editing tools to facilitate customization of the web greeting. When the sender is finished designing the web greeting, the finished web page data is stored (by software at the vendor's web site) at a site corresponding to the serial number.

When the card is received by a recipient and held in front of a Bedoop sensor, CLASS, DNS, and UID data is decoded from the card. The CLASS and DNS data are used to navigate the earlier-described server network to reach a corresponding DNS leaf node server (perhaps maintained by the Hallmark greeting card company). That leaf node server indexes a table, database, or other data structure with the UID from the Bedoop data, and obtains from that data structure the address of an ultimate web site – the same address at which the web greeting customized by the sender was stored. That address is provided by the DNS leaf node server back to the local computer, with instructions that the web page at that address be loaded and displayed (e.g., by HTML redirection). The local computer complies, presenting the customized web greeting to the card recipient.

In the just-described embodiment, in which a pre-encoded card is purchased by a sender and the web-display is then customized, the address of the web site is typically determined by the card vendor.

But this need not be the case. Likewise, the card need not be "purchased" in the typical, card-shop fashion.

To illustrate the foregoing alternatives, consider the on-line acquisition of a greeting card, e.g., by visiting a web site specializing in greeting cards. With suitable user-selection (and, optionally, customization), the desired card can be printed using an ink-jet or other printer at the sender's home. In such case, the Bedoop data on the card can be similarly customized. Instead of leading to a site determined by the card vendor, the data can lead to the sender's personal web page, or to another arbitrary web address.

To effect such an arrangement, the sender must arrange for a DNS leaf node server to respond to a particular set of Bedoop data by pointing to the desired web page. While individuals typically will not own DNS servers, internet service providers commonly will. Just as AOL provides simple tools permitting its subscribers to manage their own modest web pages, internet service providers can likewise provide simple tools permitting subscribers to make use of DNS leaf node servers. Each subscriber may be assigned up to 20 UIDs. The tools would permit the users to define a corresponding web address for each UID. Whenever a Bedoop application led to that DNS leaf node server, and presented one of those UIDs, the server would instruct the originating computer to load and present the web page at the corresponding web address.

Prior to customizing the greeting card, the sender uses the tool provided by the internet service provider to store the address of a desired destination web address in correspondence with one of the sender's available UIDs. When customizing the greeting card, the sender specifies the Bedoop data that is to be encoded, including the just-referenced UID. The greeting card application encodes this data into the artwork and prints the resulting card. When this card is later presented to a Bedoop system by the recipient, the recipient's system loads and displays the web page specified by the sender.

Commerce in Bedoop Resources

In the just-described arrangement, internet service providers make available to each subscriber a limited number of UIDs on a DNS server maintained by the service. Business enterprises typically need greater Bedoop resources, such as their own DNS IDs (or even their own CLASS ID(s).

While variants of the Bedoop system are extensible to provide an essentially unlimited number of CLASS IDs and DNS IDs, in the illustrated system these resources are limited. Public service, non-profit, and academic applications should have relatively generous access to Bedoop resources, either without charge or for only a modest charge. Business enterprises, in contrast, would be expected to pay fees to moderate their potentially insatiable demand for the resources. Small businesses could lease blocks of UIDs under a given CLASS/DNS ID. Larger businesses could acquire rights to entire DNS IDs, or to entire CLASS IDs (at commensurately greater fees).

Web-based systems for assigning DNS IDs (and CLASS IDs) can be modeled after those successfully used by Internic.com, and now Networksolutions.com, for registration of internet domains. The user fills out a web-based form with names, addresses, and billing information; the system makes the

necessary changes to all of the hidden system infrastructure – updating databases, routing tables, etc., in servers around the world.

Controlled-Access ID

Just as the above-described embodiment employed an ink-jet printer to produce a customized-Bedoop greeting card, the same principles can likewise be applied to access-control objects, such as photo-IDs.

Consider an employment candidate who will be interviewing at a new employer. The candidate's visit is expected, but she is not recognized by the building's security personnel. In this, and many other applications, arrangements like the following can be used:

The employer e-mails or otherwise sends the candidate an access code. (The code can be encrypted for transmission.) The code is valid only for a certain time period on a given date (e.g., 9:00 a.m. – 11:00 a.m. on June 28, 1999).

Upon receipt of the access code, the candidate downloads from the web site of the state Department of Motor Vehicles the latest copy of her driver's license photo. The DMV has already encoded this photo with Bedoop data. This data leads to a state-run DNS leaf node server 56. When that server is presented with a UID decoded from a photograph, the server accesses a database and returns to the inquiring computer a text string indicating the name of the person depicted by the photograph.

The candidate incorporates this photo into an access badge. Using a software application (which may be provided especially for such purposes, e.g., as part of an office productivity suite such as Microsoft Office), the photo is dragged into an access badge template. The access code emailed from the employer is also provided to this application. On selecting "Print," an ink-jet printer associated with the candidate's computer prints out an access badge that includes her DMV photo and her name, and is also steganographically encoded in accordance with the employer-provided access code.

The name printed on the badge is obtained (by the candidate's computer) from the DMV's DNS server, in response to Bedoop data extracted from the photograph. (In this application, unlike most, the photograph is not scanned as part of a Bedoop process. Instead, the photograph is already available in digital form, so the Bedoop decoding proceeds directly from the digital representation.)

For security purposes, the access code is not embedded using standard Bedoop techniques. Instead, a non-standard format (typically steganographic) is employed. The embedding of this access code can span the entire face of the card, or can be limited to certain regions (e.g., excluding the region occupied by the photograph).

On the appointed day the candidate presents herself at the employer's building. At the exterior door lock, the candidate presents the badge to an optical sensor device, which reads the embedded building access code, checks it for authenticity and, if the candidate arrived within the permitted hours, unlocks the door.

Inside the building the candidate may encounter a security guard. Seeing an unfamiliar person, the guard may visually compare the photo on the badge with the candidate's face. Additionally, the

guard can present the badge to a portable Bedoop device, or to one of many Bedoop systems scattered through the building (e.g., at every telephone). The Bedoop system extracts the Bedoop data from the card (i.e., from the DMV photograph), interrogates the DMV's DNS server with this Bedoop data, and receives in reply the name of the person depicted in the photograph. (If the Bedoop system is a telephone, the name may be displayed on a small LCD display commonly provided on telephones.)

The guard checks the name returned by the Bedoop system with the name printed on the badge. On seeing that the printed and Bedoop-decoded names match (and optionally checking the door log to see that a person of that name was authorized to enter and did so), the security guard can let the candidate pass.

It will be recognized that the just-described arrangement offers very high security, yet this security is achieved without the candidate ever previously visiting the employer, without the employer knowing what the candidate looks like, and by use of an access badge produced by the candidate herself.

Variants of such home-printed badge embodiments find numerous applications. Consider purchasing movie- or event-tickets over the web. The user can print an access ticket that has an entry code embedded therein. On arriving at the theater or event, the user presents the ticket to an optical scanning device, which decodes the entry code, checks the validity of same, authorizes the entry, and marks that entry code as having been used (preventing multiple uses of tickets printed with the same code).

Another Controlled Access ID

A great variety of access control systems can be implemented using the present technology. The foregoing is just one example.

Another application employs an ID card, Bedoop technology, and proximity detection technology (commonly known as RFID).

The ID card can be a badge or the like having a steganographically-encoded photograph of the bearer. The card further includes a proximity ID device, such as an unpowered electronic circuit that is excited and detected by a radiant field from an associated proximity detector, providing a unique signature signal identifying a particular individual.

The building can be provided with an image sensor (such as a video camera or the like), an associated Bedoop detection system, and the proximity detector. When a user wearing the badge approaches, the proximity detector signals the camera to capture image data. The Bedoop detection system identifies the badge photograph (e.g., by clues as are described in the prior applications, or without such aids), captures optical data, and decodes same to extract the steganographically-embedded data hidden therein. The access control system then checks whether the badge ID discerned from the proximity sensor properly corresponds to the Bedoop data extracted from the photograph on the badge. If so, access is granted; if not, the data is logged and an alarm is sounded.

By such arrangement, premises security is increased. No longer can proximity-based access badges be altered to substitute the picture of a different individual. If the photo is swapped, the

proximity system ID and the embedded photo data will not match, flagging an unauthorized attempted access.

The same principles are applicable in many other contexts – not limited to RF-based proximity detection systems. For example, the data decoded from the photograph can be compared against other forms of machine-sensed personal identification associated with the badge. These include, but are not limited to, bar code IDs, mag-stripe ID cards, smart cards, etc. Or the comparison can be with an identification metric not associated with the badge (e.g., retinal scan, voice print, or other biometric data).

Ink-Jet Printing

In the foregoing discussions, reference has been made to use of ink-jet printing as a means for providing steganographically encoded indicia on substrates. The following discussion expands on some of the operative principles.

The basic physics and very low level analog electronic operation of ink-jet printers (sometimes termed bubble-jet printers) are ideally suited to support very-light-tint background digital watermarking on any form of substrate. (Watermarking through apparent "tinting" of substrates is discussed in published specification WO0007356, corresponding to US application 09/127,502.) In general, the statement, "if you can print it with an ink jet printer, you can watermark it" is largely accurate, even for (perhaps especially for) simple text documents. Indeed, there is a degree of flexibility and control in the ink-jet printing realm that is not as generally available in more traditional printing technologies, such as commercial offset printing and other plate-based technologies. (This is not to say that ink-jet has better quality than plate-based technologies; it has more to do with the statistics of ink droplets than anything else.) Heavier tint backgrounds are possible as well, where the continuum ranges from very light background tinting, where the casual observer will see "white paper," all the way through heavily inked patterned backgrounds, and photographs themselves, and everything in between.

In some embodiments, the ink-jet driver software is modified to provide lower-level control of individual droplet emission than is provided in existing printer drivers, which are naturally optimized for text and graphics. In some such embodiments, the "watermarking" print mode is another option from which the user can select (e.g., in addition to High Quality, Econo-Fast, etc.), or the selection can be made automatically by application software that is printing watermarked data.

In more sophisticated embodiments, the watermark data is applied to the printer driver software independently of the other image/text data. The printer driver is arranged to eject droplets in the usual print density for the image/text data, and at a more accurately-controlled, finer density for the separately-applied watermark data. (The latter may be effected as a slight modulation signal on the former.) This arrangement provides for essentially transparent integration into existing printer environments – no one need worry about the watermarking capability except the software applications that specifically make use of same.

Consumer Marking of Web-Based Materials

Various items of printed media can originate off the web, yet be printed at home. Examples include movie tickets, coupons, car brochures, etc. Bedoop data can be added, or modified, by the software application or by the printer driver at the time of printing. (Alternatively, the Bedoop data can be customized to correspond to the user before being downloaded to the user's system for printing.)

One advantage to Bedoop-encoding printed images locally, as opposed to Bedoop-encoding the image files prior to downloading for local printing, is that the encoding can be tailored in accordance with the particular properties of the local printer (e.g., to increase robustness or decrease visibility) – properties not generally known to a remote server.

In one particular example, the UID field in the Bedoop data can be written with a value that serves as an index to a database of user profiles, permitting later systems to which the printed item is presented to personalize their response in accordance with the profile data.

In another example, the UID field serves an authentication purpose, e.g., to verify that the printed medium actually was printed at a particular place, or by a particular user or at a particular time.

Coffee Mug

At retail coffee outlets, customers commonly order the same drink day after day ("half-decaf, short, skinny latte"). Some customers present personal coffee mugs to the cashier, preferring the sensation of ceramic or metal to paper, and avoiding the trash/recycle dilemma.

The drinker's "regular" order can be Bedoop-encoded either on the mug itself or, more commonly, on an adhesive label applied to the mug. The encoding can be in addition to other aesthetic imagery (e.g., artwork or a photo), or the marking can be purely data. Labels the size of postage stamps may be used.

On handing the mug to the cashier, the customer can simply say "the regular." The cashier passes the mug in front of the optical scanning device of a Bedoop system associated with the cash register. The system steganographically decodes the data and provides the corresponding order ("half-decaf, short, skinny latte"), either textually or audibly (e.g., by a voice synthesizer) to the cashier or the barrista. The cash register system also knows the current price of the requested drink, and rings up the charge accordingly.

Labels of the type described can be available to the cashier on pre-printed rolls, just as with other adhesive stickers, or can be printed on-demand. (Small label printers may be best suited in the latter case, given space constraints in retail outlets.) Customers ordering drinks for personal mugs may be invited to take a label corresponding to their just-ordered drink and apply it to their mug for future use.

In variants on this basic theme, the mug label can be further encoded (or a supplemental label can be provided and encoded) with electronic payment information, such as the customer's credit card number, or the number of a debit account maintained by the coffee merchant for that customer. When the mug is scanned for the drink order, the system likewise detects the payment information and charges

the corresponding fee to the appropriate account. (For security reasons, the system may be arranged so that the mug cannot be used to authorize more than, say $5 of coffee drink purchases per day.)

In another variant on this theme, the system maintains an electronic log of coffee purchases made by the customer and, in accordance with then-prevailing marketing considerations, rewards the customer with a free drink after 8 or 12, etc., drinks have been purchased.

In still another variant on this theme, regular customers who use Bedoop-labeled mugs can participate in periodic promotions in which, for example, every N^{th} such customer is rewarded with a cash or merchandise prize. Bells go off when the Nth mug is scanned. (N can be a fixed number, such as 500, or can be a random number – typically within a known range or with a known mean.)

Warping and Focus Issues

The coffee cup is an example of a non-planar object. Another is soft drink cans. Special issues can arise when encoding and decoding markings on such objects. For example, when sensing such an object with a camera or the like, part of the image will be out of focus due to differing distances from the camera to different parts of the can surface.

While parts of an image sensed from a non-planar object, such as a can, may be out of focus, they still convey useful image data. The out of focus areas are just blurred – as if filtered by a low pass filter. But to make use of this information, a further complication must first be addressed: warping.

When viewed from a camera, the planar artwork with which the can is wrapped becomes warped. Portions of the can nearest the camera appear at a nominal full scale, while areas successively further around the can curvature (as viewed from the camera) appear progressively more and more spatially compressed. Regardless of the watermarking technology being employed, the physical warp of the can's surface is likewise manifested as a warping of the encoded watermark data.

On way of handling this issue is to pre-warp the watermark pattern to account for this optical distortion.

In watermarking techniques that operate directly on luminance values, the grid by which the watermark is applied can be pre-distorted to counteract the subsequent optical distortion of the artwork as it is perceived on the cylindrical can. Consider a Pepsi or Coke can. A virtual center line may pass through the center of the logo artwork (the "front" of the can), and serves as a center line of one of the watermark gridded tiles. On either side of this center line the grid is successively stretched. This stretching is computed so that, when viewed by a camera, the watermark grid has the appearance of being uniformly rectilinear, instead of being successively compressed towards the apparent edge of the can, as would otherwise be the case.

An illustration of such an approach is shown in the Figures. Fig. 17 shows an unwarped grid – as would commonly be used in watermarking planar objects. Fig. 18 shows the same grid – prewarped to account for optical distortion due to can curvature. The artwork (e.g., label) center-line is shown by the dotted lines.

More typically the grid is square rather than rectangular. Moreover, the illustrated distortion contemplates that the depicted grid spans +/- 90 degrees from the can front. Also, the grid is typically smaller (e.g., one inch on a side), so several grids are tiled adjacent each other in a span of +/- 90 degrees.) Still further, the illustrated pre-warping is based on an infinite projection (i.e., the can surface as viewed from a distance of infinity – encompassing a full +/- 90 degrees from the center line). More typically, the warp would be computed based on a finite projection – using a typical lens-to-object distance (e.g., 2-24 inches), resulting in a view that encompasses less than a full +/- 90 degree range from the center line.

The illustrated grid is pre-warped only in the horizontal direction, and only in accordance with a curvature-induced geometrical distortion. Another apparent geometrical distortion is also present – one due to different parts of the can being further from the camera. The further away, the smaller the appearance. Accordingly, grid elements expected to be positioned further from the camera should be made commensurately larger in order to pre-compensate for this distance-induced geometrical distortion. Such distance-induced geometrical distortion is manifested equally in the horizontal and vertical directions. Thus, a more accurate pre-warp would also progressively swell the grid cells both in vertical and horizontal dimensions at progressive displacements from the center line, so as to counter-act the further-looks-smaller effect. Fig. 19 shows the basic nature of such a pre-warp.

The degree of this latter pre-warping will be heavily dependent on the distance from the camera lens to the front of the can. If the distance is on the order of two inches, the further-looks-smaller effect will be much more pronounced that if the distance is a foot or more. In the latter case, the distance to the most remote portion of the imaged object may be 110% the distance to the closest portion, whereas in the former case, the ratio may be more on the order of 200%.

The illustrated pre-warping is exemplary of that which may be applied when the watermark is applied in the pixel domain using a grid pattern. It is geometrical pre-warping – i.e., in the spatial domain. Other watermarking approaches would naturally require pre-warping of other sorts, corresponding to the anticipated warping of the watermark data representation. For example, watermarking techniques that rely on changing image coefficients in transformed domains would require different adjustments. Conceptually these adjustments are the same (i.e., resulting in an apparent image having the intended watermark information), but the manifestation is not susceptible to illustration like that given in Figs. 17 and 18 (i.e., since transform coefficients are being changed - rather than grid layout, warping in a transform domain - rather than in a spatial domain, would be required).

Although the foregoing description focused on pre-warping the image, the problem can be handled otherwise. If a rectilinear watermark – not pre-warped – is applied to a cylindrical can, the watermark detector can apply an unwarping operation to counteract the applicable distortion. That is, the detector can virtually remap the raw pixel data to effectively stretch the pixels away from the center line to restore them to their proper rectilinear relationship.

In one embodiment, the sensed image data is first trial-decoded without unwarping – assuming the imaged subject is planar. If no watermark is detected, the same data (or a subsequent frame of image

data) is trial-unwarped to see if perhaps the data so yields a readable watermark. Several successive unwarpings of different characters may be tried. In some embodiments, a detector may continuously cycle through several different unwarping functions (including no unwarping) to try and happen on an unwarping function that permits a watermark be discerned from the image data.

If the application permits, the user may specify the shape of the object so that a single, or limited range, of unwarping functions is applied. Or the user can simply provide a gross cue to the detector (e.g., by selecting between "magazines" or "grocery products' on a user interface associated with the watermark detector). In the former case, the medium is known to be flexible and may assume random simple curvatures other than planar. In such case the detector may spend most of its time trying to decode the watermark assuming the imaged page is planar, and occasionally try applying one of four or eight different unwarping functions as would be appropriate if the magazine page were slightly drooping in different directions. In the latter case, grocery products are generally fairly unflexible and thus have relatively predictable shapes - most commonly planar or cylindrical. In such case the detector may spend half its time trying to decode assuming the object is planar, and spend the other half of its time cycling among a variety of cylindrical unwarping functions.

While the foregoing discussion particularly addressed image watermarking, counterparts of these principles are likewise applicable to audio watermarking.

Smart Elevators

In accordance with another embodiment, a building elevator is provided with one or more optical capture devices. Each device examines monitors the contents of the elevator chamber, looking for Bedoop encoded objects, such as ID badges.

On sensing a Bedoop-encoded object, the elevator can determine – among other data – the floor on which the wearer's office is located. The system can then automatically direct the elevator to that floor, without the need for the person to operate any buttons. (The elevator's button panel can be provided with a new, override button that can be operated to un-select the most recently selected floor(s), e.g., in case a user wants to travel to a different floor.)

To aid in identification, the Bedoop objects (e.g., badges) can be colored a distinctive color, permitting the system to more easily identify candidate objects from other items within the optical capture devices' field of view. Or the object can be provided with a retro-reflective coating, and the elevator can be equipped with one or more illumination sources of known spectral or temporal quality (e.g., constant infra red, or constant illumination with a single- or multi-line spectrum, or a pulsed light source of known periodicity; LEDs or semiconductor lasers, each with an associated diffuser, can be used for each the foregoing and can be paired with the image capture devices). Other such tell-tale clues can likewise be used to aid in object location. In all such cases, the optical capture device can sense the tell-tale clue(s) using a wide field of view sensor. The device can then be physically or electronically steered, and/or zoomed, to acquire a higher resolution image of the digitally-encoded object suitable for decoding.

Magazines

Magazine (and newspaper) pages can be steganographically encoded with Bedoop data to provide another "paper as portal" experience. As with the earlier-described office document case, the encoded data yields an address to a computer location (e.g., a web page) having the same, or related, content.

In one exemplary embodiment, the blank magazine page stock is Bedoop-encoded prior to printing. The watermarking can be performed by high speed ink-jet devices, which splatter a fine pattern of essentially imperceptible ink droplets across each page. Each page can be differently watermarked so that, on decoding, page 21 of a magazine can be distinguished from page 22 of the same magazine (and page 106 of the June 21, 1999, issue can be distinguished from page 106 of the June 28, 1999, issue). If desired, each page can be further segregated into regions – either in accordance with the actual boundaries of articles that will later be printed on the pages, or in a grid pattern, e.g., of 3 columns across by 5 rows high. Each region conveys a distinct Bedoop code, permitting different portions of the page to lead to different web data.)

After watermarking and printing, the pages thus produced are bound in the usual fashion with others to form the finished magazine. (Not all pages in the magazine need to be watermarked.)

Of course, the watermarking can be effected by processes other than ink-jet printing. For example, texturing by pressure rollers is another option well suited for the large volumes of paper to be processed. Or the artwork presented in the advertisement can be digitally watermarked using commercial watermarking software (as is available, e.g., with Adobe Photoshop and Corel image editing products).

On presenting a magazine to the optical scanner device of a Bedoop-compliant computer, the computer senses the Bedoop data, decodes same, and launches a web browser to an internet address corresponding to the Bedoop data. If the magazine page is an advertisement, the internet address can provide information complementary to the advertisement. For example, if the magazine page is an advertisement for a grocery item, the Bedoop data can identify a web page on which recipes that make use of the advertised item are presented. If the magazine page includes a photo of a tropical beach, the Bedoop data can lead to a travel web page (e.g., hosted by Expedia or other travel enterprise) that presents fare and lodging information useful to a reader who wants to vacation at the illustrated beach. (The fare information can be customized to the reader's home airport by reference to user profile data stored on the user's computer and relayed to the web site to permit customization of the displayed page.)

The data to which the Bedoop data leads needn't be static; it can be updated on a weekly, daily, or other basis. Thus, if a months-old magazine page is presented to a Bedoop device, the resultant data can be up-to-the-minute. The linked data can include audio and/or video presentations.

In the case of advertising, the inclusion of Bedoop data increases the value of the ad to the advertiser, and so merits a higher charge to the advertiser from the magazine publisher. This higher

charge may be shared with the enterprise(s) that provides the Bedoop technology and infrastructure through which the higher value is achieved.

Business Card Applications

Conventional business cards can be steganographically encoded with Bedoop data, e.g., by texturing, watermark tinting, ink-jet splattering, text steganography, etc. As with many of the earlier-described embodiments, the steganographic encoding is tailored to facilitate decoding in the presence of arbitrary rotation or scale distortion of the card introduced during scanning. (Some such techniques are shown, e.g., in applicant's earlier patents and publications identified above. Various other techniques are known to artisans.)

When a recipient of a business card holds it in front of a Bedoop sensor, the operating system on the local system launches a local Bedoop application. That local Bedoop application, in turn, establishes an external internet connection to a remote business card server. The address of that server may already be known to the local Bedoop application (e.g., having been stored from previous use), or the local Bedoop system can traverse the above-described public network of DNS servers to reach the business card server.

A database on the business card name server maintains a large collection of business card data, one database record per UID. When that server receives Bedoop data from a local Bedoop system, it parses out the UID and accesses the corresponding database record. This record typically includes more information than is commonly printed on conventional business cards. Sample fields from the record may include, for example, name, title, office phone, office fax, home phone, home fax, cellular phone, email address, company name, corporate web page address, personal web page address, secretary's name, spouse's name, and birthday. This record is transmitted back to the originating Bedoop system.

The local Bedoop system now has the data, but needs further instruction from the user as to how it should be processed. Should a telephone number be dialed? Should the information be entered into a personal contact manager database (e.g., Outlook) on the local system? Etc.

In an exemplary embodiment, the local system presents the available choices to the user, e.g., by textual prompts, synthesized voice, etc. The user responds by manipulating the business card in a manner prompted by the system (e.g., move down to telephone office; move up to telephone at home; move right to access corporate web page; move left to access personal web page; rotate left to enter certain elements from the database record (filtered in accordance with a template) into personal contact manager database, etc.. The local Bedoop system responds accordingly.

Some card givers may choose to make additional information available to card recipients -- information beyond that known in prior art contact-management software applications. For example, one of the choices presented by a local Bedoop system in response to presentation of a business card may be to review the card-giver's personal calendar. (The card-giver can maintain his or her personal calendar on a web-accessible computer.) By such arrangement, the card-recipient can learn when the card-giver may be found in the office, when appointments might be scheduled, etc., etc.

Typically, access to this web-calendar is not available to casual web browsers, but is accessible only in response to Bedoop data (which may thus be regarded as a form of authentication or password data).

Some users may carry several differently-encoded cards, each with a different level of access authorization (e.g., with different UIDs). Thus, some cards may access a biographical page without any calendar information, other cards may access the same or different page with access enabled to today's calendar, or this week's calendar, only, and still other cards (e.g., the "spouse" card) may access the same or different page with access enabled for the card-giver's complete calendar. The user can distribute these different cards to different persons in accordance with the amount of personal information desired to be shared with each.

In accordance with a related embodiment, the database record corresponding to Bedoop business card data can include a "now" telephone number field. This field can be continually-updated throughout the day with the then-most-suitable communications channel to the card-giver. When the card-giver leaves home to go to the office, or leaves the office for a trip in the car, or works a week at a corporate office in another town, etc., this data field can be updated accordingly. (A pocket GPS receiver, with a wireless uplink, can be carried by the person to aid in switching the "now" number among various known possibilities depending on the person's instantaneous position.) When this database record is polled for the "now" number, it provides the then-current information.

Consider a Bedoop-enabled public telephone. To dial the phone, a business card is held in front of the Bedoop sensor (or slid through an optical scanner track). The phone interrogates the database at the business card server for the "now" number and dials that number.

To update the any of the fields stored in the database record, the card giver can use a special card that conveys write-authorization privileges. This special card can be a specially encoded version of the business card, or can be another object unique to the card-giver (e.g., the card-giver's driver's license).

The reference to business cards and personal calendars is illustrative only. Going back a century, "calling cards" were used by persons whose interests were strictly social, rather than business. The just-discussed principles can be similarly applied. Teenagers can carry small cards to exchange with new acquaintances to grant access to private dossiers of personal information, favorite music, artwork, video clips, etc. The cards can be decorated with art or other indicia that can serve purposes wholly unrelated to the Bedoop data steganographically encoded therein.

Gestural Input

A Bedoop system can determine the scale state, rotation state, X-Y offset, and differential scale state, of an object by reference to embedded calibration data, or other techniques. If the scan device operates at a suitably high frame rate (e.g., five or ten frames per second), change(s) in any or all of these four variables can be tracked over time, and can serve as additional input.

In an earlier-discussed example, moving an object to the left or right in front of the Bedoop scanner caused a left- or right-positioned button in a dialog box to be selected. This is a change in the X-Y offset of the scanned object. In that earlier example, moving the object inwardly towards the camera caused the selected button to be activated. This is a change in the scale state of the scanned object.

In similar fashion, twisting the object to the left or right can prompt one of two further responses in a suitably programmed Bedoop application. (This is a change in the rotation state.) Likewise, tilting the object so that one part is moved towards or away from the camera can prompt one of two further responses in the application. (This is a change in the differential scale state.)

In the business card case just-discussed, for example, the card can be held in front of the Bedoop scanner of a computer. If the card is twisted to the left, the computer opens a web browser to a web page address corresponding to Bedoop data on the card. If the card is twisted to the right, the computer opens an e-mail template, pre-addressed to an e-mail address indicated by the card.

In other examples, twisting an object to move the right edge towards the scanner can be used to effect a right mouse click input, and twisting the object to move the right edge away from the scanner can be used to effect a left mouse click input.

Simultaneous changes in two of these four positioning variables can be used to provide one of four different inputs to the computer (e.g., (a) twisting left while moving in; (b) twisting left while moving out; (c) twisting right while moving in; and (d) twisting right while moving out). Simultaneous changes to three or all four of these variables can similarly be used to provide one of eight or sixteen different inputs to the computer.

Simultaneous manipulations of the object in two or more of these modes is generally unwieldy, and loses the simple, intuitive, feel that characterizes manipulation of the object in one mode. However, a similar effect can be achieved by sequential, rather than simultaneous, manipulation of the card in different modes (e.g., twist left, then move in). Moreover, sequential manipulations permit the same mode to be used twice in succession (e.g., move in, then move out). By such sequential manipulations of the object, arbitrarily complex input can be conveyed to the Bedoop system.

(It will be recognized that a digitally-encoded object is not necessary to the gestural-input applications described above. Any object (talisman) that can be distinguished in the image data can be manipulated by a user in the manners described above, and an appropriate system can recognize the movement of the object and respond accordingly. The provision of digital data on the object provides a further dimension of functionality (e.g., permitting the same gesture to mean different things, depending on the digital encoding of the object being manipulated), but this is not essential.

Moreover, even within the realm of digitally-encoded gestural talismans, steganographic encoding is not essential. Any other known form of optically-recognizable digital encoding (e.g., 1D and 2D bar codes, etc.) can readily be employed.

In an illustrative embodiment, a business card or photograph is used as the talisman, but the range of possible talismans is essentially unlimited.

Dynamic gestures are not the only communications that can be effected by such talismans. Static positioning (e.g., presenting the talisman at different orientations) can alternatively be employed.

Consider a magazine advertisement. When presented to the sensor with the top of the page up, a first response can be invoked. If the page is presented at a rotation of 90 degrees, a second response can be invoked. Similarly with 180 degrees rotation (i.e., upside down), and 270 degrees rotation. The Bedoop detector can detect these different rotational states by reference to attributes of the watermark signal discerned from the magazine page (e.g., by reference to the rotation state discerned from the subliminal grid signal detailed in applicant's prior patents).

Gestural Decoding Module

There are various ways in which the Bedoop system's decoding of gestural input can be effected. In some Bedoop systems, this functionality is provided as part of the Bedoop applications. Generally, however, the applications must be provided with the raw frame data in order to discern the gestural movements. Since this functionality is typically utilized by many Bedoop applications, it is generally preferable to provide a single set of gestural interpretation software functions (commonly at the operating system level) to analyze the frame data, and make available gestural output data in standardized form to all Bedoop applications.

In one such system, a gestural decoding module tracks the encoded object within the series of image data frames, and outputs various parameters characterizing the object's position and manipulation over time. Two of these parameters indicate the X-Y position of the object within current frame of image data. The module can identify a reference point (or several) on the object, and output two corresponding position data (X and Y). The first represents the horizontal offset of the reference point from the center of the image frame, represented as a percentage of frame width. A two's complement representation, or other representation capable of expressing both positive and negative values, can be used so that this parameter has a positive value if the reference point is right of center-frame, and has a negative value if the reference point is left of center frame. The second parameter, Y, similarly characterizes the position of the reference point above or below center-frame (with above-being represented by a positive value). Each of these two parameters can be expressed as a seven-bit byte. A new pair of X, Y parameters is output from the gestural decoding module each time a new frame of image data is processed.

In many applications, the absolute X-Y position of the object is not important. Rather, it is the movement of the object in X and Y from frame-to-frame that controls some aspect of the system's response. The Bedoop application can monitor the change in the two above-described parameters, frame to frame, to discern such movement. More commonly, however, the gestural decoding module performs this function and outputs two further parameters, X' and Y'. The former indicates the movement of the reference point in right/left directions since the last image frame, as a percentage of the full-frame width. Again, this parameter is represented in two's complement form, with positive values representing movement in the rightward direction, and negative values representing movement in the leftward

direction. The later parameter similarly indicates the movement of the reference point in up/down directions since the last frame.

The scale, differential scale, and rotation states of the object can be similarly analyzed and represented by parameters output from the gestural decoding module.

Scale state can be discerned by reference to two (or more) reference points on the object (e.g., diagonal corners of a card). The distance between the two points (or the area circumscribed by three or more points) is discerned, and expressed as a percentage of the diagonal size of the image frame (or its area). A single output parameter, A, which may be a seven-bit binary representation, is output.

As with X-Y data, the gestural decoding module can likewise monitor changes in the scale state parameter since the last frame, and product a corresponding output parameter A'. This parameter can be expressed in two's complement form, with positive values indicating movement of the object towards the sensor since the last frame, and negative values indicating movement away.

A differential scale parameter, B, can be discerned by reference to four reference points on the object (e.g., center points on the four edges of a card). The two points on the side edges of the card define a horizontal line; the two points on the top and bottom edges of the card define a vertical line. The ratio of the two line lengths is a measure of differential scale. This ratio can be expressed as the shorter line's length as a percentage of the longer line's length (i.e., the ratio is always between zero and one). Again, a two's complement seven-bit representation can be used, with positive values indicating that the vertical line is shorter, and negative values indicating that the horizontal line is shorter. (As before, a dynamic parameter B' can also be discerned to express the change in the differential scale parameter B since the last frame, again in two's complement, seven bit form.)

A rotation state parameter C can be discerned by the angular orientation of a line defined by two reference points on the object (e.g., center points on the two side edges of a card). This parameter can be encoded as a seven-bit binary value representing the percentage of rotational offset in a clockwise direction from a reference orientation (e.g., horizontal). (The two reference points must be distinguishable from each other regardless of angular position of the object, if data in the full range of 0 – 360 degrees is to be represented. If these two points are not distinguishable, it may only be possible to represent data in the range of 0-180 degrees.) As before, a dynamic parameter C' can also be discerned to express the change in the rotation state parameter C since the last frame. This parameter can be in seven bit, two's complement form, with positive values indicating change in a clockwise rotation

The foregoing analysis techniques, and representation metrics, are of course illustrative only. The artisan will recognize many other arrangements that can meet the needs of the particular Bedoop applications being served.

In the illustrative system, the Bedoop application programs communicate with the gestural decoding module through a standardized set of interface protocols, such as APIs. One API can query the gestural input module for some or all of the current position parameters (e.g., any or all of X, Y, A, B, and C). The module responds to the calling application with the requested parameter(s). Another API can query the gestural input module for some or all of the current movement data (e.g., any or all of X',

Y', A', B' and C'). Still another API can request the gestural decoding module to provide updated values for some or all of the position or movement data on a running basis, as soon as they are discerned from each frame. A complementary API discontinues the foregoing operation. By such arrangement, all of the gestural data is available, but the Bedoop application programs only obtain the particular data they need, and only when they ask for it.

In Bedoop applications that communicate with external servers, just the Bedoop data (i.e., CLASS, DNS, and optionally UID) may initially be sent. If the remote server needs to consider gestural data in deciding how to respond, the remote server can poll the local Bedoop system for the necessary data. The requested gestural data is then sent by the local Bedoop system to the remote server in one or more separate transmissions.

In other embodiments, since the gestural data is of such low bandwidth (e.g., roughly 56 bits per image frame), it may routinely and automatically be sent to the remote computer, so that the gesture data is immediately available in case it is needed. In an illustrative implementation, this data is assembled into an 8-byte packet, with the first byte of the packet (e.g., the X parameter) being prefixed with a "1" sync bit, and subsequent bytes of the packet being prefixed with "0" sync bits. (The sync bits can be used to aid in accurate packet decoding.)

In some embodiments, it is useful to provide for an extension to the normal 64-bit Bedoop length to accommodate an associated packet of gestural data. This can be effected by use of a reserved bit, e.g., in the UID field of the Bedoop packet. This bit normally has a "0" value. If it has a "1" value, that indicates that the Bedoop data isn't just the usual 64 bits, but instead is 128 bits, with the latter 64 bits comprising a packet of gestural data.

Similar extension protocols can be used to associate other ancillary data with Bedoop data. A different reserved bit in the UID field, for example, may signal that a further data field of 256 bits follows the Bedoop data – a data field that will be interpreted by the remote computer that ultimately services the Bedoop data in a known manner. (Such bits may convey, e.g., profile data, credit card data, etc.) The appended data field, in turn, may include one or more bits signaling the presence of still further appended data.

Grandmothers

It is a common complaint that computers are too complex for most people. Attempts to simplify computer-user interaction to facilitate use by less experienced users usually serve to frustrate more experienced users.

In accordance with this aspect of the present technology, the sophistication of a computer user is steganographically indicated on a talisman used by that user to interact with the system. The computer detects this steganographically-encoded data, and alters its mode of interacting with the user accordingly.

Consider internet browser software. Experienced users are familiar with the different functionality that can be accessed, e.g., by various drop-down menus/sub-menus, by the keyboard

shortcuts, by the menus available via right-clicking on the mouse, by manipulating the roller mouse scroll wheel and scroll button, etc., etc. Grandmothers of such users, typically, are not so familiar.

Although gestural interfaces hold great promise for simplifying user-computer interaction, the same dichotomy between experienced users and inexperienced users is likely to persist, frustrating one class of user or the other.

To help close this gap, a computer system can respond to gestures in different manners, depending on the expertise level indicated by encoding of the talisman. For an expert user, for example, the gestural interface active in the internet browser software may display the stored list of Favorite web addresses in response to tipping the left edge of the talisman towards the optical sensor. Once this list is displayed, the expert user may rotate the talisman to the right to cause the highlighting to scroll down the list from the top. Rotating the talisman to the left may scroll the list of Favorites up from the bottom. The speed of scrolling can be varied in accordance with the degree of rotation of the talisman from a default orientation.

In contrast, for the novice user, these talisman manipulations may be confounding rather than empowering. Tipping the left edge of the talisman towards the sensor may occur as often by mistake as on purpose. For such users, a more satisfactory interface may be provided by relying on simple X-Y movement of the talisman to move an on-screen cursor, with a movement of the talisman towards the sensor to serve as a selection signal (i.e., like a left-mouse click).

(In the example just-cited, the expert user summoned a list of Favorite web sites. Different "Favorites" lists can be maintained by the computer – each in association with different talismans. A husband who uses one talisman is provided a different "Favorites" list than a wife who uses a different talisman.)

Printed Pictures

A printed photograph can be steganographically encoded with Bedoop data leading to information relating to the depicted person (e.g., contact information, biographical information, etc.).

Such a photograph can be presented to a Bedoop sensor on a telephone. In a simple embodiment, the telephone simply processes the Bedoop data to obtain a corresponding default telephone number, and dials the number. In other embodiments, various options are possible, e.g., dial home number or dial work number. On presenting the photograph to the telephone, for example, moving the photo to the left may dial the person at home, while moving the photo to the right may dial the person at work.

As telephones evolve into more capable, multi-function devices, other manipulations can invoke other actions. In a computer/telephone hybrid device, for example, rotating the photo counterclockwise may launch a web browser to an address at which video data from a web cam at the pictured person's home is presented. Rotating the photo clockwise may present an e-mail form, pre-addressed to the e-mail address of the depicted person. Moving the photo to the right may query a database on the system

for other photographs depicting the same individual or subject, which can be presented in response to further user input. Etc.

In this and other embodiments, it is helpful for the Bedoop device to prompt the user to aid in manipulating the object. This can be done audibly (e.g., "move photo left to dial at home") or by visual clues (e.g., presenting left- or right-pointing arrows).

Bedoop data in photographs can also be used to annotate the photographs, as with notes on the back of a photograph, or printed under the photograph in a photo album. The Bedoop data can lead to a remote database, where the photograph owner is permitted to enter a textual (or audio) narrative in association with each photograph's UID. Years later, when some of the names have been forgotten, the photograph can be positioned in front of a Bedoop sensor, and the system responds by providing the annotation provided by the photograph owner years earlier.

Drivers Licenses and Other Cards

Drivers licenses, social security cards, or other identity documents may be encoded by the issuing authority with Bedoop data that permits access to the holder's personal records over the web. On presenting the document to a Bedoop system, the system directs a web browser to a private address corresponding to data encoded on the document. At that address, the holder of the document can review governmental records, such as state or federal tax return data, social security entitlements, etc., as well as privately-maintained records, such as credit records, etc. User selection among various functions can be effected by spatial manipulation of the document. (Entry of additional data, such as social security number or mother's maiden name, may be required of the user to assure privacy in case the document is lost or stolen.)

By manipulating a driver's license in front of a Bedoop sensor, a user can request renewal of the driver's license, and authorize payment of the corresponding fee.

Bank cards (debit, credit, etc.) can similarly be encoded with Bedoop data to permit the holder to access bank records corresponding to the bank card account. (Entry of a PIN code may be required to assure privacy.)

Such documents can also be used to access other personal data. One example is e-mail. A traveler might pause at a Bedoop kiosk at an airport and present a driver's license. Without anything more, the kiosk may present email that is waiting for the traveler on an associated display screen.

On recognizing a driver's license, the kiosk can access a remote site (which may be maintained by the Department of Motor vehicles, another government entity, a private entity, or by the traveler), authenticating the operation by presenting Bedoop data encoded on the license, and obtain information that the person has pre-approved for release in response to such authorized access. This information can include e-mail account and password information. Using this information, the kiosk queries the corresponding e-mail server, and downloads a copy of recently received mail for presentation at the kiosk. (A user-entered PIN number may be required at some point in the process, e.g., in querying the

remote site for sensitive e-mail password data, before presenting the downloaded e-mail for viewing, etc., to ensure privacy.)

Other cards carried in wallets and purses can also be encoded to enable various functions. The local sandwich shop that rewards regular customers by awarding a free sandwich after a dozen have been purchased can encode their frequent-buyer card with Bedoop data leading to the shop's web-based sandwich delivery service. Or the frequent-buyer card can be eliminated, and customers can instead wave their business card or other identity document in front of the shop's Bedoop sensor to get purchase credit in a tally maintained by the sandwich shop's computer.

Food stamps, health insurance cards, and written medical prescriptions, can likewise be encoded with digital data to enable the provision of new functionality.

At large trade shows, such as COMDEX, vendors needn't publish thick, glossy brochures to hand out to visitors. Instead, they may print various stylish promo cards for distribution. When later presented to a Bedoop sensor, each card leads to a web-based presentation – optionally including persuasive video and other multi-media components. The user can be prompted to provide data to customize, or focus, the presentation to the user's particular requirements. If the user wants further information, a request can be made by the click of a mouse (or the twist of a card).

Prizes and Product Promotions

Product packaging (e.g., Coke cans, Snapple bottles, Pepsi 12-pack boxes) can be encoded for contest purposes. The encoding can be customized, item to item, so that selected items – when Bedoop scanned – are recognized to be the one in a hundred that entitles the owner to a cash or merchandise prize. A remote server to which the item's Bedoop data is provided queries the user for contact information (e.g., address, phone number) so the prize can be awarded or, for smaller prizes, the system can print out an award certificate redeemable at local merchants for products or cash. Once a winning item is identified to the remote server, its UID on the server is marked as redeemed so that the item cannot later be presented to win another prize.

In other such embodiments, all of the items are encoded identically. Winners are determined randomly. For example, during a contest period, persons around the world may present Coke cans to Bedoop systems. The corresponding Bedoop application on each user computer submits Bedoop data to a corresponding web address. The user's e-mail address may also be included with the submission. As this data is relayed to the corresponding server computer(s), every N^{th} set of data is deemed to be a winner, and a corresponding award notification or prize is dispatched to the Bedoop system from which the winning set of data originated.

The server computer that receives such contest submittals from client Bedoop systems can be arranged to prevent a single user from bombarding the server with multiple sets of data in an attempt to win by brute force. (This may be done, for example, by checking the included e-mail address or received IP address, and not considering a data submittal if the same address was encountered in data submitted within the past hour. Similar anti-brute-force protection can be provided on the user's computer,

preventing, e.g., repeated contest data to be sent more frequently than once per hour. More sophisticated anti-brute-force measures can of course be provided.)

Non-planar product packaging, such as cylindrical soda cans, present certain optical issues in encoding and decoding which are detailed further below.

Product Information and Ordering

Product packaging and product advertisements can be encoded with Bedoop data that, when presented to a Bedoop system, initiates a link to a web page from which that product can be purchased, or more information obtained. Once the link has been established, the user can be instructed to manipulate the object in different of the earlier-described modes to effect different functions, e.g., move towards camera to order the product; move away from camera for product information. If the object is moved towards the camera to effect an order, the user can be prompted to further manipulate the object to specify delivery options (e.g., rotate left for overnight mail, rotate right for regular mail). If the object is moved away from the camera to request product information, the user can be promoted to further manipulate the object to specify the type of information desired (e.g., rotate left for recipes, rotate right for FDA nutritional information, move up for information on other products in this family, move down to send an email to the product manufacturer).

Credit card or other customer billing information, together with mailing address information, can be stored in a profile on the Bedoop system, and relayed to the transactional web site either automatically when a purchase action is invoked, or after the user affirms that such information should be sent (which affirmation may be signaled by manipulation of the packaging or advertisement in one of the earlier-described modes). Other modes of payment can naturally be employed.

Computer Access Cards

This disclosure earlier considered access cards used to gain access to secure buildings. Related principles can be used in conjunction with computer access.

A driver's license, employee photo ID, or other such document can be presented to a Bedoop sensor on a computer. The computer recognizes the user and can take various steps in response.

One response is to log onto a network. Another is to set load a user profile file by which the computer knows how to arrange the desktop in the user's preferred manner. By manipulating the Bedoop-encoded object, the user can further vary the environment (e.g., rotate left to launch standard business productivity applications and software development applications; rotate left to launch lunchtime diversions – stock update, recreational games, etc.)

Hotel rooms are increasingly providing computer services. By presenting a driver's license, a Bedoop-equipped computer in a hotel room can link to a remote site indicated by the Bedoop data, obtain preference data for that user, and launch applications on the hotel computer in an arrangement that mimics that user's familiar work computer environment.

Audio/Video Disks, Software, and Books

Bedoop data can be conveyed by indicia or texturing on the surfaces of CD and DVD disks, on the labels (or authenticity certificates) or inserts or artwork for same, on the enclosures for same (e.g., jewel box, plastic case, etc.), on book dust jackets, on book pages, etc. Any of these objects can be presented to a Bedoop device to establish a link to a related web site. The consumer can then manipulate the object (or otherwise choose) to select different options.

For music, one option is to receive MP3 or other clips of songs by the same artist on other CDs, or of songs from other artists of the same genre. Another is to view music video clips featuring the same artist. Still another is to order tickets to upcoming concerts by that artist. In-store kiosks can permit tentative customers to listen to sample tracks before they buy.

Similar options can be presented for video DVDs. In the case of video, this can include listings of other movies with the same director, with the same star(s), etc. In the case of software, the options can include advisories, bug fixes, product updates and upgrades, etc. Naturally, the user can make purchases from these sites, e.g., of other music by the same artist, other videos with the same star, software upgrades, etc.

Similar options can be accessed using Bedoop data associated with printed book materials.

Children learn the mechanics of turning book pages at an early age. Children learn to look at pictures on the pages of a book and they enjoy hearing the story that is related to the images. Generally, adults read the words and the child follows along looking at the pictures. Children enjoy repeatedly hearing the words of a story. The association of seeing pictures and repeatedly hearing the words is an excellent mechanism for learning to read and learning to enjoy books.

Embedded digital watermark data can automate the above process so that a child can see the pictures, and hear the words independently. Such an arrangement provides enjoyment for the child while teaching reading and love for books, and at the same time giving the child independence and familiarity with an automated mechanism.

More particularly, images in the book, or the paper substrates of the pages, contain digital watermarks. As a child turns the pages of the book, a camera captures the image and an associated computer reads the watermark. The watermark is then used to index a data store – either local or remote – to obtain text corresponding to the page being viewed. A text-to-speech converter is then employed to voice the text to the child. (Alternatively, the data store can contain digitized speech, rather than simple text – permitting different story characters to be given different voices, etc.) Thus, as a child turns the pages of the book, the child hears the words that are printed on the page. By turning pages, the child controls the process. The child will naturally make an association between the printed words and the words that are played by the computer.

Ad Tracking

Advertisers commonly use different advertisements for the same product or service, and employ means to track which ad is more effective within which demographic group. Bedoop can provide such functionality.

Consider a travel service web site that is promoting Hawaiian vacations. Bedoop data from several advertisements can lead consumers to the site.

Identical advertisements can be placed in several different magazines. Each is encoded with a different Bedoop UID. By monitoring the UIDs of the Bedoop inquiries to the site, the travel service can determine which magazines yield the highest consumer response (e.g., per thousand readers).

Likewise, within a single magazine, two or more advertisements may be encoded with Bedoop data leading to the site – again, each with a different UID. Again, analysis of the UIDs used in accessing the site can indicate which advertisement was the more effective.

The two UIDs in the foregoing examples may both lead to the same internet destination, or may lead to different destinations.

The instantaneous nature of the internet links permits advertisers to learn how consumer responses to print advertisements vary with time-of-day, yielding information that may assist in making ads for certain products more effective.

More elaborate variants and combinations of the foregoing are, of course, possible, If the consumers provide personal information in response to the ads (either by permitting access to pre-stored personal profile data, or by filling in web-based forms, or by manipulation of the ad (e.g., "please move the ad towards your Bedoop sensor if you drank coffee this morning")), still richer statistical data can be gleaned.

Rolodex of Cards

Bedoop-encoded business cards as detailed above can be accumulated and kept near the telephone or computer in a Rolodex-like arrangement. If a refrigerator ice-maker malfunctions, a homeowner can find the card for the appliance repairman used a few years ago, and present it to a Bedoop sensor. A link is established to the repairman's company (e.g., web site or via telephone). At a web site, the repairman may provide basic information, such as hours of availability, current fee schedule, etc. The homeowner may select an option (by card gesture or otherwise) to invoke a teleconference (e.g., NetMeeting) to consult about the problem. Or the homeowner may select another option to send e-mail. Still a further option may permit the homeowner to schedule a house call on the repairman's weekly calendar. Still a further option may permit the homeowner to view one or more short videos instructing customers how to fix certain common appliance problems.

Stored Value Cards

An electronic money system (e.g., of the sort detailed in US application 60/134,782, filed May 19, 1999) may encode Bedoop data on a card that leads to storage at which random-number tokens

(which represent increments of money) are stored. Presenting the card to a Bedoop system launches an application that reads and encrypts the tokens and forwards the encrypted data to the clearinghouse computer of the corresponding bank to learn their remaining value. There the tokens are decrypted and checked for validity (but not redeemed). The bank computer responds to the Bedoop system, indicating the remaining value of the tokens on the card.

For security reasons, the storage containing the random-number tokens should not be generally accessible. Instead, the user must provide authentication data indicating authorization to gain access to that information. This authentication data may be a PIN code. Or the user may provide authentication by presenting a second Bedoop-encoded object, e.g., a driver's license to the Bedoop system. (Many other Bedoop systems may advantageously use, or require the use of, two or more Bedoop objects – either presented one after the other, or all at the same time. The Bedoop system can provide visual or audible prompts leading the user to present the further Bedoop object(s) as necessary.

Ski Lift Tickets

In accordance with another embodiment, ski lift tickets are Bedoop encoded to provide various functionality.

For example, instead of buying a lift ticket good for a day, a skier may purchase a ticket good for eight lifts. This data is encoded on the ticket, and sensed by a Bedoop sensor at each lift. The sensors are networked to a common server that tracks the number of lifts actually purchased, and updates the number as used. The skier is informed of the number of rides remaining on entering or leaving the lift. Statistical data can be collected about trail usage (e.g., N% percent of skiers ski all day along just two lifts, etc.).

Off the slopes, back at home, the used lift ticket may be presented to a Bedoop sensor to obtain current snow conditions and lift hours, or to review trail maps, or to order ski vacation packages. If the ticket is encoded with the owner's name, UID, or other information of commercial/marketing interest, local merchants may give the bearer discounts on selected goods in response to Bedoop scanning of the ticket and recovery of such information.

REI Membership Cards

Membership cards for certain stores can be Bedoop-encoded to provide added value to the member. For outdoor gear stores such as REI, presentation of the card to a Bedoop sensor can lead to a library of USGS maps, to web pages with current fishing and hunting regulations, etc. Naturally, the store's on-line ordering site is just a quick twist away.

Theme Park Tickets

Theme park tickets can be encoded with the age and gender of the visitor, and with additional data permitting the experience to be customized (e.g., from a roster of theme park personalities, the visitor's favorite is Indiana Jones). Throughout the park are kiosks to which the visitor can present the

ticket to orchestrate the visit to follow a particular story line. Some kiosks issue premiums matching the age/gender of the recipient.

Car Keys

Car keys (or key ring fobs) are Bedoop encoded. When the car is taken to a shop for service, the mechanic presents the key to a Bedoop sensor, and thereby obtains the car's maintenance history from a remote server on which it is maintained. At home, the key can be presented to a Bedoop sensor and manipulated to navigate through a variety of automotive-related web sites.

In some embodiments, the Bedoop-encoded object is not used to navigate to a site, but is instead used to provide data once a user's computer is otherwise linked to a web site. A user surfing the web who ends up at a car valuation site can present a key to the Bedoop scanner. The Bedoop data is used to access a remote database where the make, model, options, etc., of the car are stored. This data is provided to a database engine that returns to the user the estimated value of the car.

While visiting a mechanic's web site, presentation (and optionally manipulation) of a key or key ring fob can be employed to schedule a service appointment for the car.

Fashion Coordination

Some department stores and clothing retailers offer "personal shoppers" to perform various services. For example, a customer who is purchasing a dress may ask a personal shopper for assistance in selecting shoes or accessories that complement the dress.

A Bedoop-encoded garment tag on the dress can be employed to obtain similar assistance. In response to such a tag, a Bedoop system can query a database to obtain a mini-catalog of clothes and accessories that have previously been identified as complementing the dress identified by the tag. These items can be individually displayed on a screen associated with the system, or a virtual model wearing the dress - together with one or more of the recommended accessories - can be synthesized and depicted. The shopper may quickly review the look achieved by the model wearing the dress with various different pairs of shoes, etc., by repeatedly activating a user interface control (by mouse, touch screen, or garment tag gestures) to cycle through different combinations.

A shopper's credit card can be Bedoop-encoded so as to lead Bedoop systems of particular stores (i.e., stores pre-authorized by the shopper) to a profile on the shopper (e.g., containing size information, repeat purchase information, return history, style/color preferences, etc.).

Credit Card Purchases

When a consumer visits a commercial web site and wishes to purchase a displayed product, the transaction can be speeded simply by presenting a Bedoop-encoded credit card to a Bedoop sensor on the user's computer. The Bedoop data on the card leads to a database entry containing the credit card number and expiration date. The Bedoop application then sends this information (optionally after encrypting same) to the web site with instructions to purchase the depicted product.

(Impulse purchases are commonly deterred by the hurdles posed between the purchase impulse and the completed purchase. This and other Bedoop applications aid in reducing such hurdles.)

Product Marketing

Bedoop data relating to one product or service can be used to cross-market others products and services. Consider a consumer who purchases a pair of golf shoes. The box is Bedoop encoded. By presenting the box to a Bedoop system, the consumer is linked to a web page that presents various promotional offers. The consumer may, for example, elect to play a free round of golf at one or more identified local golf courses, or print a coupon for ten percent off any order of socks from an on-line sock merchant. (Various means can be employed to prevent multiple redemptions from a single box. One is a serial number that is tracked by the web page or cross-marketed merchant, and only honored once. Another is identification data corresponding to the consumer that is tracked to prevent multiple redemptions.)

Product tags can likewise be Bedoop-encoded. A tag from an article of Nike apparel can lead to the Nike on-line store, where the user can buy more merchandise. If the tag is from a soccer jersey, a certain tag manipulation (e.g., rotate left) may lead the user to a special-interest soccer page, such as for the World Cup. A tag on a golf glove may lead to a website of a local golf course. Twist left to reserve a tee time; twist right to review course maps and statistics. Bedoop kiosks can be provided in retail stores to let consumers use the Bedoop features.

Travel Planning Services

After making a reservation at a resort, a consumer is typically mailed (by email or conventional mail) various confirmation information. If not already printed, the consumer can print this information (e.g., a confirmation card).

Bedoop-encoding on the printed object can lead to web-based information relating to the reservation (e.g., reservation number, the consumer's name, arrival/departure dates, etc.). If the consumer wishes to make dinner or golf reservations, this object is presented to a Bedoop system – either at the user's home, at an airport kiosk, etc. The system recognizes the object type and encoded data, and establishes a link to a remote computer that provides various information and scheduling services for the resort. By manipulating the object (or otherwise) the consumer selects desired dinner and golf tee times. The system already has the reservation number (indexed by the UID), so tedious provision of such data is avoided.

In some embodiments, the remote computer is not maintained by the resort, but is rather maintained by an independent travel service. (The travel service may also maintain the DNS leaf node server.) The computer can present a web page (branded by the travel service or not) that offers the scheduling options desired by the user, and also presents links to other information and services (e.g., offering entry tickets to nearby attractions, and advertising nearby restaurants).

Airline tickets (or e-ticket confirmations) can be similarly encoded with Bedoop data. These items may be presented to Bedoop systems – at a traveler's home or in airports – to permit review and changing of travel itinerary, reserve hotels and rental cars, secure first-class upgrades, check the airplane's seating arrangement, review frequent flier status, scan tourist information for the destination, etc.

Movie Tickets

As indicated earlier, movie tickets can be encoded with Bedoop data identifying, e.g., the movie title and date. When a movie viewer returns home, the ticket stub can be presented to a Bedoop system. One of the options presented by the corresponding Bedoop application can be to launch a pay-per-view screening of the just-seen movie at a discounted rate. Another is to download the movie onto a writeable DVD disk at the viewer's home, perhaps serialized to permit playback only on that viewer's DVD player, or enabled for only a few playbacks, etc. (again, likely for a discounted fee). Still another option is to present web-delivered video clips from the movie. Another is to offer related merchandise for purchase, possibly at discount to retail. (These features may be available for only a limited period after the date encoded on the ticket stub.) Another is to alert the consumer to upcoming movies of the same genres, or with the same director or stars, or released by the same studio. Still another is to direct a web browser to an on-line ticket merchant for tickets to other movies. The consumer may navigate among these options by manipulating the ticket stub, or otherwise.

The same, or related, options can likewise be provided in response to Bedoop data detected from a book jacket presented to a Bedoop system.

Video Recording

A video recording device can be programmed to record a broadcast program by presenting a Bedoop sensor with a printed promotion for the program (e.g., an advertisement in a newspaper or TV Guide). Bedoop-encoded within the printed document is data by which the Bedoop system (which may be built into the video recorder or separate) can set the recording time, date, and channel.

Set Top Boxes

Many entertainment-related applications of Bedoop data can be implemented using television set top boxes. Such boxes include processors, and typically include a return channel to a control facility. The provision of a Bedoop chip and optical sensor can vastly increase the functionality these devices presently provide.

Special Event Tickets

Consider a ticket to a basketball game. By presenting the ticket to a Bedoop system, a user may access the web site of either team so as to review recent scores and statistics. The user may also obtain a web-based virtual tour of the arena, and review seating maps. The view of the playing field as seen from

the user's seat location may be presented. Tickets for upcoming games may be ordered, as well as pay-per-view games and team souvenirs. For high-priced tickets, the user may be entitled to premium web features, such as on-line text-, audio-, or video-chat session with a team star on the day before the game.

Unlike conventional tickets, Bedoop-encoded tickets need not limit the user to a predetermined seat. While the ticket may be printed with a nominal seat, the user may present the ticket to a Bedoop sensor and access a web site at which a different seat can be reserved. On attending the event, the consumer presents the ticket to a Bedoop sensor that reads the ticket UID and looks up the seat assignment most-recently picked by the consumer. It then prints a chit entitling the consumer to take the seat earlier selected from the transactional web site.

Signet Rings

Signet rings have historically been used to indicate a person's identity or office. Such rings, or other items of personal jewelry, can be encoded with Bedoop data (either by texturing or printing) and presented as necessary to Bedoop systems. The extracted Bedoop data can lead to a secure web site indicating the person's name and other information (i.e., a web site that has anti-hacking measures to prevent illicit change of the stored identification information). Such a signet ring can be presented to Bedoop systems that require a high-confidence confirmation of identity/authorization before proceeding with a Bedoop function.

Tattoos

Temporary tattoos are well known and typically include an ink or printed film that is transferred to a wearer's skin through some application process (e.g., wetting or otherwise). The artwork on the tattoo can be arranged to steganographically encode Bedoop data, facilitating machine recognition of the persons (or objects) tattooed. Youths can compile a contacts database simply by snapping digital photos of friends using an imaging-capable personal digital assistant. Such a computer device can decode the watermark, access a corresponding web dossier of information on the person photographed, and add such information to a contacts database.

E-Paper

While it is doubtless evident that a great variety of printing technologies can be employed in Bedoop applications, it should be noted that e-paper can be employed as well. E-paper, developed by Nicholas K. Sheridon of Xerox, and mass produced by 3M, is a thin layer of transparent plastic in which millions of small beads, somewhat like toner particles, are dispersed. The beads, each contained in a fluid -filled cavity, are free to rotate within those cavities. The beads are "bichromal," with hemispheres of contrasting color (e.g. black and white). Under the influence of a voltage applied to the surface of the sheet, the beads rotate to present one colored side or the other to the viewer. A pattern of voltages can be applied to the surface in a bit-wise fashion to create images such as text and pictures. The image persists

until new voltage patterns are applied to create new images. The reader is presumed familiar with the US patents issued to Sheridon on this technology.

It will further be recognized that epaper can be used to convey digital data according to essentially any known watermarking method, and is also suitable for conveying digital information in data glyph form.

Post-It® Notes

Pads of Post-It® notes, or other pads of paper, can be marked by the manufacturer (either by texturing, watermarked tinting, ink-jet spattering, etc.) to convey steganographic data (e.g., Bedoop data). When such a note is presented to a Bedoop system, the system may launch an application that stores a snapshot of the note. More particularly, the application may mask the note-portion of the image data from the other image data, virtually re-map it to a rectangular format of standardized pixel dimensions, JPEG-compress the resulting image, and store it in a particular computer subdirectory with a name indicating the date of image acquisition, together with the color and/or size of the note. (These latter two data may be indicated by data included in the Bedoop payload.) If the color of the note is indicated by digital data (e.g., in the file name), then the image itself may be stored in grey-scale. When later recalled for display, the white image background can be flooded with color in accordance with the digital color data.

The Bedoop system may buffer several past frames of image data. When the object is recognized as a Post-It note whose image is to be saved, the system may analyze several such frames to identify the one best-suited for storage (e.g., check the spatial frequency content of the note as imaged in each frame, to identify the one with the finest detail), and store that one.

When a Post-It note is recognized by the Bedoop system, the system may emit a confirmation tone (or other response) to indicate that the object has been recognized, but not immediately execute the snapshot operation. Instead, the system may await a further instruction (e.g., gesture) to indicate what operation is desired.

By moving the note towards the sensor, for example, the user can signal that a snapshot operation is to be performed. (This closer presentation of the note may also permit the imaging system to capture a more detailed frame of image data.)

By moving the note away, the system may respond by reading, decompressing, and displaying the six most-recently stored Post-It note images, in tiled fashion, on the computer screen. The individual notes can be displayed at their original dimensions, or each can be re-sized to fill the full height or width of a tile. A user interface control (responsive to gestures, mouse operation, keyboard scroll arrows, etc.) allows the user to scroll back in time to any desired date.

The full 64-bit Bedoop payload of other embodiments may not be needed for Post-It notes. In the just-given example, for example, the Bedoop system responds to all Post-It notes in the same fashion. Thus, an abbreviated Bedoop format that indicates simply 'I'm a Post-It note, yellow, size 3" x 3"' can suffice. The twelve bit CLASS ID, with eight further bits to indicate color/size combinations, may be

sufficient. Reducing the payload permits it to be more robustly encoded on small objects. (As noted below, Bedoop decoding systems can look for several different data formats/protocols in trying to extract Bedoop data from an object.)

Alignment of Documents for Other Purposes

While the just-described pre-marked paper triggered a Bedoop response when presented to a Bedoop sensor (i.e., take a snapshot of the paper), the markings can be used for purposes other than to trigger Bedoop responses.

Regardless of the particular data with which the paper is encoded, the embedded subliminal graticules, or other steganographically-encoded registration data, can be used by other applications to correct misalignment of scanned data. In a photocopier, for example, a document need not be placed exactly squarely on the glass platen in order to yield a properly-aligned photocopy. The scanner scans the skewed document and then detects the steganographic registration markings in the resulting scan data. This data is then processed to virtually re-register same, so that the registration markings are in a desired alignment. The processed scan data is then provided to the xerographic reproduction unit to yield a photocopy in which the skew effect is removed.

The same technique is likewise applicable to video recorders, digital cameras, etc. If such a device images an object (e.g., a photograph) with steganographic registration markings, these markings can be used as a guide in re-registering the resulting data to remove mis-alignment effects.

Postal Mail Information

Many contexts arise in which data to be presented to a consumer is valuable only if timely. The postal service mail is ill-suited for some such information due to the latency between printing a document, and its ultimate delivery to a recipient. Bedoop principles, however, allow the recipient to take a postal object that was printed well before delivery, and use it on receipt (i.e., present to a Bedoop system) to receive up-to-the-minute information. In this and other embodiments, the Bedoop data can also uniquely identify the addressee/recipient/user, so the web site can present data customized to that user.

Distributors of printed advertising can reward Bedoop-driven consumer visits to their web sites by issuing digital tokens or coupons that can be redeemed for premiums, cash-back, etc. Every millionth visitor wins a million pennies (with appropriate safeguards, e.g., preventing more than one entry an hour).

Classes of Bedoop Encoding

The above-described embodiments focused on use of Bedoop data after decoding. Additional insight may be gained by examining the earlier part of the process – encoding.

Encoding can be performed in many contexts, which may be conceptualized as falling into three broad classes. The first is static marking, in which a document designer, pre-press service bureau,

advertising agency or the like embeds Bedoop data. The second is dynamic marking, in which automated systems encode, or vary, Bedoop data "on the fly." Such systems can tailor the Bedoop data to particularly suit the context, e.g., to the moment, place, user, etc. The third is consumer marking, in which Bedoop data is added to a document at the time of printing.

The second class of encoding enables features not available from the first. Consider an American Express travel web page with information about travel to Hawaii. A DNS leaf node server points to this page in response to certain Bedoop data – e.g., data encoded in a magazine photograph of a Hawaiian beach scene.

Actually, all Bedoop data having a certain CLASS and DNS ID may lead to this web page, irrespective of the UID data. If the magazine photo is encoded with a particular "don't care" UID field (e.g., 111111111111111111111111), this may signal the originating Bedoop system – or any intervening system through which the Bedoop data passes – that arbitrary data can be inserted in the UID field of that Bedoop packet. The originating Bedoop system, for example, can insert a dynamically-configured series of bits into this field. Some of these bits can provide a profile of the user to the remote server, so that the Bedoop response can be customized to the user. (The user would naturally pre-approve information for such use so as to allay privacy concerns.)

As one example, the local Bedoop system can set the least significant bit of the UID field to a "0" if the user is male, or to a "1" if the user is female. The next four bits can indicate the user's age by one of sixteen age ranges (e.g., 3 or less, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15, 16-17, 18-20, 21-24, etc.).

Alternatively, or in addition, the local Bedoop system can stuff the don't-care UID field (all of it, or in part) with signature data tending to uniquely identify the local Bedoop system (e.g., system serial number, a hash code based on unchanging data unique to that system, etc.) By reference to such data, the remote server can identify repeat visits by the same user, and can tailor its responses accordingly (e.g., by recalling a profile of information earlier entered by the user and stored at the remote server, avoiding the need for data re-entry).

More on Optical Input Devices

It is expected that image input devices will soon become commonplace. The provision of digital cameras as built-in components of certain computers (e.g., the Sony Vaio laptops) is just one manifestation of this trend. Another is camera-on-a-chip systems, as typified by U.S. Patent 5,841,126 and detailed in Nixon et al., "256x256 CMOS Active Pixel Sensor Camera-on-a-Chip," IEEE J. Solid-State Circuits, Vol. 31(12), pp. 2046-2051 (1996), and Fossum, "CMOS Image Sensors: Electronic Camera-on-a-Chip," IEEE Transactions of Electron Devices, vol. 44, No. 10, Oct. 1997. Still another is head-mounted cameras (as are presently used in some computer-augmented vision systems). These and other image input devices are all suitable for use in Bedoop systems.

Camera-on-a-chip systems can be equipped with Bedoop detector hardware integrated on the same chip substrate. This hardware can be arranged to find and decode Bedoop data from the image data – notwithstanding scale, rotation, differential scaling, etc. Gestural decoding can also be provided in

hardware, with the resulting data output in packet form on a serial output bus. Such a chip can thus provide several outputs – image data (either in raw pixel form, or in a data stream representing the image in one of various image formats), 64 bits of Bedoop data (serially or in parallel), and decoded gesture data.

In other embodiments, the Bedoop detector (and/or the gestural decoder) can be on a substrate separate from the camera system.

To accommodate different Bedoop data formats and protocols, the hardware can include RAM or ROM in which different format/protocol information is stored. (These different formats/protocols can relate, e.g., to Bedoop systems employing different data payload lengths, different subliminal grids, different encoding techniques, etc.) As the Bedoop system stares out and grabs/analyzes frames, each frame can be analyzed in accordance with several different formats/protocols to try and find a format/protocol that yields valid Bedoop output data.

Movable Bedoop Sensors

Although the illustrated Bedoop systems are generally stationary, they need not be so. They can be portable. Some such systems, for example, employ palmtop computers equipped with optical sensor arrays. If the palmtop is provided with live network connectivity (e.g., by wireless), then Bedoop applications that rely on remote computers can be implemented just as described. If the palmtop is not equipped with live network connectivity, any Bedoop applications that rely on remote computers can simply queue such communications, and dispatch same when the palmtop next has remote access (e.g., when the palmtop is next placed in its recharger and is coupled to a modem through which internet access can be established).

Another variant is a Bedoop sensor with a 1D or 2D photosensor array (e.g., CCD or CMOS) that is movable around a desk or other work-surface, like a mouse. Such a sensor can be coupled to the associated computer by cabling, or a wireless interface can be used. The peripheral may be arranged for placement on top of an item in order to read digital data with which the object is marked. (Built-in illumination may be needed, since the device would likely shadow the encoding.) Some forms of such peripherals are adapted to serve both as general purpose digital cameras, and also as Bedoop sensors.

Such a peripheral would find many applications. In "reading" a magazine or book, for example, it may be more intuitive to place a Bedoop reader "on" the object being read, rather than holding the object in the air, in front of a Bedoop sensor. This is particularly useful, e.g., when a magazine page or the like may have several differently-encoded Bedoop sections (corresponding to different articles, advertisements, etc.), and the user wants to assure that the desired Bedoop-encoded section is read.

The "bookmark" paradigm of internet browsers might be supplemented with paper bookmarks, e.g., Bedoop data encoded on one or more pages of paper. To direct a browser to a particular bookmarked destination, the peripheral is simply placed on top of the page (or part thereof) that is marked with the corresponding Bedoop data. A user may print a "map" comprised of postage stamp-sized regions tiled together, each of which regions represents a favorite web destination.

Such a map may be printed on a mouse pad. Indeed, mouse pads with certain maps pre-encoded thereon may be suitable as promotional materials. A company may offer to print a family photograph on such a pad. Encoded within the photograph or the pad texture are addresses of web sites that have paid a fee to be accessible in this manner on a user's desk.

In this and other contexts, it will be recognized that the gestural input concepts detailed earlier involve relative movement between the sensor and the encoded object. In most of the earlier examples, the sensor is stationary, so gesticulation is effected by moving the object. Naturally, if the sensor is moveable (e.g., as a mouse or cell phone), the gestural movement can be effected by moving the sensor instead.

One particular embodiment of the arrangement detailed above a modified version of the Microsoft IntelliMouse with IntelliEye technology. That device includes a multi-element optical sensor integrated on an IC with various detector and processing circuitry, operating in conjunction with a short focal length imaging lens and an LED illumination source (all available from Agilent, as detailed below). The circuitry tracks movement of patterns across the sensor's field of view, by which the mouse's movement can be deduced. The Microsoft product collects 1500 data sets per second – a frame rate much higher than is generally needed for the present applications. Some such embodiments combine the functionality of a mouse with that of a Bedoop image sensor.

Such a mouse-like peripheral can omit the buttons and position-sensing features commonly provided on traditional mice, yielding a simple desk-facing palm camera that generates frames of data corresponding to a small area under the sensor portion of the mouse. More typically, however, the peripheral includes the buttons, roller wheels, and/or X-/Y- position sensing arrangements of traditional mice so that button and positional forms of data input can be exploited in interacting with the Bedoop application.

The optical data collected by the sensor can be processed within the peripheral's processor to extract the steganographically encoded binary Bedoop data therefrom. Or this processing burden can be undertaken by the associated computer system, with the peripheral simply processing and formatting the raw sensor data into sequential frames of image data to be output to that system.

While scanning peripherals of the type described above are typically wired to an associated host system, wireless links (e.g., radio, infrared, ultrasonic, etc.) can of course be used, freeing the user from the constraint imposed by the cable.

Hand Scanners – More

To elaborate on the concepts introduced above, the following paragraphs particularly detail a hand scanner modeled after the Hewlett-Packard CapShare 920. The scanner may be configured for use with any type of identifier, e.g., watermark, barcode, OCR, etc.

The reader is presumed familiar with the workings of the HP CapShare scanner. Such information has been published in the technical literature, e.g., Allen, Ross R. et al, "Processes for Freehand Image Capture: HP CapShare Technology," The Society for Imaging Science & Technology

PICS Conference, pp. 43-46, March 26, 2000. The CapShare scanner employs an optical sensor tracking engine assembly, comprised of part Nos. HDNS2000 (IC sensor chip), HDNS-2100 (lens with light pipe), HDNS-2200 (LED clip), and HLMP-ED80 (639 nm LED), the use of which is detailed in Agilent Application Note 1179, all available from Agilent Technologies, Palo Alto, CA.

As shown in Fig. 13, the CapShare scanner 210 functionally includes a CPU 212, a memory 214, a linear CCD array 216, first and second 2D CCD arrays 218a, 218b, a user interface (including an LCD screen and associated buttons) 220, and an interface 222 (e.g., a serial port and an IRDA port/transceiver) to an auxiliary device 224. Although not particularly shown, each of the CCD sensors has an associated LED system for illuminating the object being imaged.

A further enhancement to the CapShare scanner is to provide a wireless internet interface for interface 222, permitting direct communication between the device 210 and the internet.

The linear sensor 216 operates in a conventional manner, acquiring successive pixilated line-scans of imagery under the scanner at a pixel data rate of about 18 Mbits/second (permitting full accuracy scanning even at instantaneous scanner motion speeds of up to 16 inches per second).

The two 2D CCDs 218a, 218b, are spaced apart, adjacent the linear sensor, and are used to track the scanner's movement. The areas scanned by these CCDs are illuminated obliquely by IR light, highlighting microscopic media surface features. The CPU identifies patterns in the surface features detected by each of these CCDs, and tracks their movement from one frame to the next to discern the movement of the two CCDs. By knowing the movement of the two CCDs, the movement of the scanner itself can be determined. This scanner motion information is used to re-map the swathed scan data acquired from the linear scanner array into composite pixel data with uniform scanline spacing. This remapped data is the final scan data that is typically provided to the end user or application.

The sizing of the linear and 2D CCD arrays is left to the designer. If 600 dpi line scan resolution is desired across a four inch scan swath, a 2400 element linear CCD would be used. The 2D CCDs are typically smaller in extent, e.g., having an aperture of 0.25 inches x 0.25 inches. The spacing of the CCD elements is selected based on the size of surface features to be tracked.

The memory 214 includes both RAM and ROM. The RAM is used both for raw data storage, and for storage of final results. The scanner's operating system, pattern matching and data processing algorithms, and other program code are stored in the ROM.

In accordance with the illustrated embodiment, the ROM code also includes instructions for examining the final-result scan data (i.e., after re-mapping) for watermark data. In one particular embodiment, this is a two-step process. The final-result data is first screened by the CPU to determine whether it has certain hallmarks associated with watermarked data (e.g., the presence of a calibration signal, as detailed in U.S. patent 5,862,260). If such hallmarks are found, a more computationally-intense watermark decoding algorithm is performed. By checking for watermark information in such a two-step process, CPU time isn't spent needlessly trying to extract a watermark from image data that apparently has no watermark.

In some embodiments, the watermark processing operation(s) occurs without user intervention – each time the raw scan data is processed and remapped into final-result form. In other embodiments, the watermark processing is invoked in response to a user command entered through the user interface 220. In still other embodiments, the watermark processing is invoked in response to a command provided to the scanner from an associated auxiliary device 224 (e.g., a local personal computer, a remote server computer, a specialized internet appliance, etc.).

In some embodiments, the decoded watermark payload data is transferred to an associated auxiliary device whenever such data is detected. In other embodiments, the data is not sent unless the auxiliary device 224 first asks for it. Such an auxiliary device request may be made by a software program that is executing on the auxiliary device, e.g., through an API call.

A watermark decoded by the scanner can be presented to the user on the scanner's LCD display 220. Or the scanner can forward the decoded watermark to a remote device 224, which can then reply with supplemental data for presentation to the user, as detailed elsewhere in this specification.

In some embodiments, the information obtained by the 2D CCDs 218a and/or 218b can be used to augment the information provided to the CPU so as to aid in the watermark detection/decoding process. For example, the 2D sensors provide 2D information immediately – without the time delay associated with remapping the 1D data from the linear CCD array into final form. This immediate 2D information may be analyzed for the presence of a calibration signal – perhaps shortening or obviating analysis for the calibration signal in the final data.

The 2D data can also be used to characterize the texture of the imaged substrate. Knowing the substrate texture allows the CPU to apply filtering or other watermark-enhancing/image enhancing steps as best fits the particular circumstance.

The 2D data also allows the CPU to assess the relative quality of different regions of line-scan data in the final scan data. In Fig. 14, an object 230 is scanned by a scanner 210 traveling an arced path, yielding successive lines of raw scan data 228. The geometry of the arc is revealed by data collected by the two 2D CCDs (which serve as motion encoders). Where the successive lines are spaced closer together (as at region A), the raw scan data is of higher resolution (relatively "oversampled"). In contrast, where the successive lines are spaced further apart (as at region B), the raw scan data is of lower resolution (relatively "undersampled"). In its screening or analysis for subtle watermark data, the CPU can be instructed to look first in region A, reasoning that the higher quality of the raw data in this region is most likely to include usable watermark information. (In some embodiments, watermark screening and/or detection may proceed by reference to the raw scan line data, rather than waiting for the data to be remapped into final form.)

The two CCDs 218a, 218b also permit various binocular processing to be performed so as to enhance, or allow for more intelligent processing, of the linear scan data. Consider, for example, the case where the image being scanned doesn't convey a perfectly planar (e.g., rectilinear) signal. The substrate could be warped, or the image may have been printed in a skewed manner, or some other transformation may have taken place that creates an image that changes orientation/scale over its extent. One such

example is shown in Fig. 15, which depicts a watermark calibration signal (here presented as an overt grid, for clarity of illustration). Each of the two 2D CCDs 218a, 218b senses a differently-oriented calibration signal. By reference to differences in the data sensed by the two spaced-apart CCDs, the CPU can infer scale, rotation, or other image transformation at intermediate points, and apply a compensation to the scan data so as to counteract such distortion.

Such compensation need not be based on a watermark calibration signal. Any other optically-sensed attribute at the two spaced-apart points may be used to infer the same, or related attributes, at intermediate positions, permitting appropriate compensation(s) to be applied.

Another application of the spaced-apart sensors 218 is to bi-optically determine the distance from the scanner to the object being imaged. Consider Fig. 16, which shows a scanner 10 with two spaced-apart CCD sensors 218a, 218b, imaging a warped object 232 (e.g., a warped paper substrate, or a curved object such as a drink can). In the depicted example, the first CCD 218a detects a very crisp image of surface texture or imagery, whereas the second CCD 218b detects an image similar to the first CCD, but blurred – as if low-pass filtered. Software instructions for CPU 212 can cause the scanner to recognize that the part of the object 232 under CCD 218a is immediately adjacent the scanner (and adjacent the nearby portion of the linear CCD array 216), whereas the part of the object under CCD 218b is spaced somewhat from the scanner.

Having information about the spacing of the object 232 from different parts of the linear sensor array permits certain compensations to be made in the data collected by the linear scanner. In the case of watermark detection, the CPU may recognize that data from the end of the linear scanner 216 remote from the object 232 will be devoid of meaningful high frequency information. In many watermark detection algorithms, the CPU can disregard data from such portion of the linear scanner – allowing it to focus on portions of the image data with the necessary high frequency components, thus producing more reliable results more quickly.

In other watermarking systems, two watermarks may be present – one conveyed in reliance on high frequency image components, and another encoded mostly with low frequency image components (i.e., in anticipation of circumstances where the object is imaged slightly out-of-focus). Upon recognizing that the linear scan data is weak in high frequency components, the CPU can be programmed to look just for the low frequency watermark data.

Just as the scanner 210 can perform watermark decoding, it can similarly perform barcode decoding. Conventional pattern-recognition algorithms can be applied by CPU 212 to either the raw or final scan data to identify barcode patterns. Once the pattern is identified, decoding is straightforward by applying known barcode alphabets. As in the watermark case, barcode decoding can be performed autonomously, or in response to user/auxiliary device command. Similarly, the decoded barcode data can be provided to the auxiliary device whenever detected, or in response to an auxiliary device query. The 2D data can likewise be used to augment the information provided to the CPU so as to aid in the barcode detection/decoding process.

In similar fashion, the above-described benefits associated by use of the two 2D CCDs can similarly be applied in the barcode context.

As earlier described, once the identifier information is extracted from the image data, internet links can be based thereon to provide supplemental information, e-commerce opportunities, etc. In many implementations, the scanner UI 220 is used to present this supplemental information to the user, e.g. by software instructions that render HTML instructions for presentation on the UI display screen. The UI controls (e.g., buttons) can likewise be used to receive user instructions and commands, for linking back to the internet.

Cell Phones as Bedoop Devices; GPS Receivers

Bedoop technology can be integrated into portable telecommunication terminals, such as cell phones (manufactured, e.g., by Motorola, Nokia, Qualcomm, and others). Such a phone can be equipped with a 1D or 2D image sensor, the output of which is applied to Bedoop decoding circuitry within the phone. This decoding circuitry can be the phone's main CPU, or can be a processing circuit dedicated to Bedoop functionality. (In this as in other embodiments, , the decoding can be effected by dedicated hardware, by decoding software executing on a general purpose CPU, etc.)

Cell phones are already equipped with numerous features that make them well suited for Bedoop operation. One is that cell phones typically include an LCD or similar screen for display of textual or graphic information, and additionally include buttons or other controls for selecting among menu options presented on the screen (e.g., by moving a cursor). Moreover, cell phones naturally include both audio input and output devices (i.e., microphone and speaker). Still further, the protocol by which cell phones transmit data includes data identifying the phone, so that such data need not be separately encoded. And finally, cell phones obviously provide ready links to remote computer systems. Collectively, these capabilities rival those of the most fully-equipped desktop computer system. Thus, essentially all of the applications detailed elsewhere in this specification can be implemented using cell phone Bedoop systems.

As with the other Bedoop systems, when Bedoop data is sensed, the phone can respond to the data locally, or it can forward same over the cellular network to a remote system (or computer network) for handling.

One application that may be invoked locally (i.e., within the phone) is the dialing of a corresponding telephone number. In some embodiments, the phone number is literally encoded as part of the Bedoop data payload. In others, the phone number is stored in a memory within the phone, and indexed in accordance with an identifier decoded from the Bedoop data.

The variety of operations that can be handled remotely is virtually limitless. Some entail interaction with the user. For example, the remote system may initially respond by presenting to the user a menu of options on the display screen (e.g., Purchase, Add to Shopping List, Request Sample, Add to Notepad, etc.) The user then responds by providing further input (e.g., by manipulating one or more buttons on the phone, by providing spoken instructions to a voice recognition sub-system within the

phone, etc.). This further data is then dispatched from the phone, and the requested action undertaken. Other operations don't require further interaction with the user, but immediately invoke a corresponding action.

While the just-described arrangement included the Bedoop decoding function within the phone, in other embodiments the image data can be transmitted from the phone and decoded at a remote location.

Reference was earlier made to GPS receivers as permitting the location of a person to be tracked, and contact information updated accordingly. GPS receivers find many other applications in Bedoop contexts. For example, the response of a Bedoop system can be tailored, or vary, in accordance with the location of the person invoking the operation. To illustrate, if a user presents a newspaper insert or coupon for a Dominos pepperoni pizza meal to the Bedoop sensor on a GPS-equipped cellular phone, the GPS data can be encoded in the Bedoop data dispatched to the Domino's Bedoop server. That server can identify, by reference to the GPS data, the location of the nearest Domino's franchise, and can forward the order to that franchisee. The franchisee, in turn, can telephone the user (by reference to telephone number data from the cell phone) to confirm the order, inquire if additional items are desired, inform the user of the final price, and to obtain the delivery address. (The latter step can be omitted; the franchisee can employ the GPS data to obtain the corresponding street address, e.g., from map data licensed through NavTech of Chicago.)

The protocols by which the Bedoop data, GPS data, and cell phone identification data are conveyed from the phone to the cellular network can take various forms; the design of such systems are familiar to those in the relevant arts. In one embodiment, the protocols by which some cell phones are now provided with email or internet access are further adapted to convey Bedoop and GPS data. The protocols for conveying telephone identification data are already well established. Once received by the cellular network, the Bedoop data can be formatted into packets, either incorporating the GPS data and telephone data into the same packet structure, or by formatting such data into separate packets accompanying the Bedoop packets.

The provision of image sensors in cell phones enables other functionality. One is the capture of still or video imagery. Such image data can be compressed (typically by lossy processes such as MPEG, JPEG, or the like, implemented with dedicated hardware CODECs) and transmitted with the audio data. The screens on such phones can likewise be used for display of incoming image or video data.

Another function enabled by image sensors in cell phones is user-verification, e.g., by retinal scanning or other optically-sensed biometrics, before the phone will permit a call to be placed. A great number of such biometric verification techniques are known.

Cell phone Bedoop sensors may not always be in communication with the cell phone network. The phone may be out of range of a cell site, or may be in operational mode in which an RF link is not then established. In such events, any Bedoop data sensed by the phone that is to be handled remotely is desirably stored locally within the phone, and queued for transmission to the cellular network the next time communication is established (a so-called "store and forward" form of operation).

Catalog Advertising

Any form of hand-held scanner - whether of the type just described or others known in the art - offers a convenient way to interact with catalog advertising. Imagine a traditional paper catalog, e.g., from L.L. Bean, Inc., or Lands End. Each image in the catalog is Bedoop-encoded with a code that identifies the depicted product (and, if necessary, the manufacturer, etc.). A user browsing through the catalog, on seeing a product of interest, places the scanner over the picture (and optionally may be required to push a button or otherwise signal to initiate further processing). The scanner detects the Bedoop data and relays it to an associated computer (optionally with data identifying the consumer). The computer polls a remote server computer maintained by the merchant, which responds with data corresponding to the item depicted in the scanned image. This returned data can include data indicating the sizes available, data indicating the colors available, data indicating the variant styles available, flag bits indicating whether each item is in stock, etc. This returned data can be presented to the consumer – typically on a display device but alternatively in audible form.

Preferably, the customer's body measurements (waist size, inseam length, neck size, etc.) are stored in a user profile, either on the local computer, at the merchant's server computer, or at the computer of a third party service provider. This allows the system to customize the data presented to the user – e.g., showing the color options and availability only for the depicted shirt in a 16 inch neck and a 34 inch sleeve length.

If necessary, the user can select among the color or style options, using the handheld input device (either buttons, gestures, etc.), or any other input device. Or the item may be one for which no further specifications are needed. In either event, once the desired product has been sufficiently specified, the user can signal the system to place the order. Payment and shipping details can be arranged through any of the great variety of techniques known in the art, e.g., by charging to a credit card number and shipping to an address on-file with the merchant.

Revenue Sharing

When a consumer presents a Bedoop-encoded object to a sensor, and as a result of the link(s) thereby established, purchases a product or service, the revenue from that transaction may be shared with the participants who made it possible. In the case of a Bedoop-encoded magazine ad, some of the participants may include (1) the photographer or graphic designer who produced artwork used in the ad; (2) the advertising agency whose creative talent led to the ad; (3) the publisher of the magazine in which the consumer encountered the ad; (4) the service provider(s) who provided the transport channel(s) between the consumer and the vendor; and (5) the service provider who maintained the server that ultimately linked the Bedoop data to the vendor's web site.

Gambling Applications

Casinos around the world deploy considerable resources each year to deter cheating. To that end, playing cards and chips used for gaming and betting could be encoded with digital watermarks and used to enhance security. In order for the application to work, playing cards and chips would be encoded with data unique to each casino, game, card deck and/or face value. Then, cameras placed above gaming tables would be used to read the information off the cards and chips. The information from the cards could be used to alert security or keep records of suspicious activity in the following ways.

A camera placed above a card gaming table (like Blackjack) could read the data encoded in the backs of the cards determining the authenticity and face value of those cards. This means the camera could catch anyone trying to replace cards after they were dealt-either by flagging cards as not being part of the deck currently in use or by flagging them as being a different face value than those dealt to the player. If a player switches cards after they are dealt, the watermark reader in the camera can alert security of the fraudulent activity.

Additionally, the data encoded in the cards can be used to track the winner(s) at the table. If the dealer and the player are in collusion, that player may be dealt winning cards on a regular, predetermined basis (based on tricky shuffling by the dealer). By watching the pattern and face value of cards that are dealt, it can be determined if a player wins at a much higher than average rate. Again, security personnel can be alerted to suspicious activity.

Cameras placed above gaming tables where chips are used (certainly not limited to card games) can be programmed to watch for watermarks in chips. Any chip that does not include the appropriate watermark can signal that a chip might be counterfeit. In another situation, the face value of the chips can be determined as they are placed on the table such that any switching of the chips after play begins will be noted.

The foregoing principles are more generally applicable to monitoring and surveillance systems employing digital watermark technology to identify monitored objects.

PART II

As noted, the following disclosure focuses on one particular application – a system for linking print media to electronic content. It should be reiterated, however, that the technology is not so limited, and may more generally be viewed as a system for linking any object (physical or electronic) to a corresponding networked or local resource.

In accordance with an exemplary application of the below-detailed technology, digital watermarking is employed to convey a plural bit identifier within print media, such as magazine advertisements or articles, direct mail coupons or catalogs, bank- or credit-cards, and business cards. This identifier is read by software in a user's computing device and forwarded to a remote database. The remote database identifies a URL corresponding to the identifier, and provides the URL back to the user's computer – permitting a browser on the user's computer to display the URL-identified web page. That web page can provide additional information or services – more timely and/or more extensive than

that provided by the print material. By such arrangement, more efficient internet navigation and access is provided to consumers, and more effective means for linking readers to e-commerce points of sale is provided to advertisers.

Before beginning a detailed exposition, it may be helpful to provide an overview of the larger system of which the present technology forms a part. As shown in Fig. 1, the larger system entails four basic processes – registering, embedding, detection and response.

Registering refers to the process of assigning an ID to an object, and associating that ID with a corresponding action or response. Additional steps can be included, such as logging the name and/or organization of the registrant, the name of the product, a description of the object and a context in which it is found (magazine, book, audio track, etc.), etc.

Embedding refers to the process of encoding of an object with a digital identifier (e.g., a watermark conveying a serial number in its payload).

Detection is the complementary operation to embedding, i.e., discerning a digital identifier from an object.

Response refers to the action taken based on the discerned identifier.

The middle two steps – embedding and detection – can employ any of myriad well-known technologies, including 1D and 2D barcodes, magnetic ink character recognition (MICR), optical character recognition (OCR), optical mark recognition (OMR), radio frequency identification (RF/ID), data glyphs, organic transistors, magnetic stripe, metadata, file header information, UV/IR identifiers, and other machine-readable indicia and techniques for associating plural-bit digital data with an electronic or physical object. The detailed embodiment employs watermarking technology, although this is illustrative only.

Referring to Fig. 2, a system 10 according to the exemplary embodiment includes an originating device 12, a router/server 14, a product handler 16, a registration database 17, and one or more remote resources 18.

The originating device 12 can take many different forms, e.g., a cell phone, a personal digital assistant (e.g., a Palm Pilot), a personal computer, a barcode scanning system, etc. For expository convenience, the embodiment is described with reference to a personal computer for device 12.

Device 12 interacts with an object 20. The object can be electronic or not. Electronic objects 20 can include computer files, representations of audio, video, or still imagery (e.g., files or in streaming form), etc. Non-electronic objects can include physical objects such as newspapers, magazine pages, posters, product packaging, event tickets, credit cards, paper currency, etc. Non-electronic objects can also include sounds produced by loudspeakers.

When used with non-electronic objects, device 12 (Fig. 2) typically includes some form of sensor or transducer 22 to produce electronic signals or data corresponding to the object. Examples include CCD- or CMOS-based optical sensors (either as part of still- or video cameras, flatbed scanners, mice, or otherwise), microphones, barcode scanners, RF ID sensors, mag stripe readers, etc. In such cases, the sensor 22 may be coupled to associated interface electronics 24, which in turn may be coupled to device driver software 26, which in turn may be coupled to one or more application programs 28.

Device driver software 26 serves as a software interface, communicating at a relatively high level with the application programs 28 (e.g., through API instructions whose content and format are standardized to facilitate application programming), and at a relatively low level with the interface electronics 24.

The detailed embodiment contemplates that the object 20 is a magazine advertisement encoded with a steganographic watermark conveying a plural bit object identifier. The watermark is hidden in the advertisement's image in a manner indiscernable to human observers, but detectable by computer analysis. That analysis is performed by a watermark detector 30.

Watermark detector 30 can be implemented in various different locations in the system of Fig. 1. Typically, the detector is implemented in the originating device 12, e.g., in the driver software 26, or in application software 28c that serves to link to external resources based on detected watermarks. But it may be implemented elsewhere, e.g., in hardware in the interface electronics 24, in an operating system associated with the device, or outside device 12 altogether. Some systems may have plural watermark detectors, implemented at different locations throughout the system.

In an illustrative system, the watermark detector is implemented in the device driver 26. Functionality of the detector is made available to the application program 28c through one or more APIs specific to watermark-related functions. One function is reading of the watermark data payload from the object 20.

The illustrated application 28c is a software program that serves to communicate the watermark data from the device 12 to the router/server 14 through one or more communications links 32 (e.g., the internet). Application 28c also receives information from the communication links 32 and presents same to the user (or otherwise uses same).

The router/server 14 is a high capacity computer including one or more CPUs, memory, disks, and I/O ports. As is familiar to artisans, the disks store operating system software and application programs, together with data, that are transferred to the memory as needed by the CPU. The router essentially serves as a middleman between the application 28c and the product handler 16. As detailed below, the router receives requests from the application, logs them in a transaction log 15, and passes them on to the appropriate product handler.

As more particularly detailed below, the handler 16 provides a response in accordance with the particular watermark payload. The response may be provided directly by the product handler to the device 12, or the handler may respond by communicating with a remote resource 18 (which may be, e.g., a data repository or service provider).

In the former case, the handler 16 may identify a URL corresponding to the watermark (using the database 17), and return the URL to the application 28c. Application 28c can then pass the URL to a web browser 28b in the device 12, and initiate a link to the internet site identified by the URL. Or the handler may have some locally stored data (e.g., audio or video, or software updates) and send it to the device 12 in response to the watermark.

In the latter case, the handler 16 does not respond directly to the device 12. Instead, the handler responds by communicating with a remote resource 18. The communication can be as simple as logging

receipt of the watermark message in a remote repository. Or it can be to authenticate device 12 (or a user thereof) to a remote resource in anticipation of a further transaction (e.g., the communication can form part of an on-line licensing or digital rights management transaction). Or the communication can request the remote resource to provide data or a service back to device 12 or to another destination (e.g., to initiate an FTP file transfer, or to request that a song selection identified by the watermark be downloaded to a user's personal music library, or to update software installed on device 12).

In still other cases, hybrids of the two foregoing cases can be employed, e.g., handler 16 can send some data back to device 12, while also communicating with a remote resource 18.

In some cases, the response returned to the device 12 by handler 16 (or a remote resource 18) can serve to trigger some further action by the device 12. For example, the response returned to device 12 can include a WindowsMedia audio file, together with a request that the device 12 launch the WindowsMedia player installed on the device. (The launching of a browser pointed to a URL is another example of such triggering.)

The illustrated product handler 16 comprises essentially the same hardware elements as the router 14, e.g., CPU, memory, etc. Although Fig. 2 shows just one product handler, several product handlers can be included in the system – either co-located of geographically distributed. Different handlers can be dedicated to different functions (e.g., serving URLs, serving music, etc.) or to different watermark sources (e.g., one responds to watermarks found in audio, another responds to watermarks found in print advertising, etc.). Further specialization may also be desirable (e.g., one handler may respond to advertising placed by Ford, another may respond to advertising placed by Chevrolet; or one handler may respond to advertising appearing in Wired magazine, another may respond to advertising appearing in Time magazine, etc.). In one particular implementation, the router 14 dispatches the incoming data to one of several handlers in accordance with (1) the vendor of the originating application 28c, and (2) the particular identity of the application 28c.

The following discussion focuses on the data exchanged between the application 28c, the router/server 14, the product handler 16, and the associated protocols, in one illustrative embodiment.

Concept of Operation

When shown a watermarked image, the application 28c analyzes the image and extracts the embedded watermark payload (more particularly detailed below) from the image. The application sends some or all of this information in a message format to the router 14.

The router 14 decodes the received message, looking for vendor and product information. Based on this information, it passes the message to a corresponding product handler 16.

The product handler receives the message and attempts to match the detected watermark serial number to a registered watermark serial number earlier stored in the database 17. If a match is found, the product handler performs the desired action. As noted, typical actions include returning a URL for web redirection, serving up an HTML page for initial user navigation, initiating software downloads, etc. If a match is not found, the product handler returns an error code and message to the application 28c. If a

match is found, but the corresponding action is unavailable, incomplete, inactive or invalid, the product handler returns an error code and message to the calling application.

A generalized view of the foregoing is provided in Fig. 4.

(Note that while the system may concentrate on a certain type of object 20, and a certain vendor's application 28c, the architecture is constructed to support accessing product handlers from other vendors and corresponding to other objects. This concept makes the system suitable as a clearinghouse for processing all machine-readable indicia on web-enabled devices.)

An exemplary detection and response cycle is illustrated below.

User	Application	Router	Product Handler
Shows object to sensor 22			
	Acquires watermark Creates message packet Sends packet to product handler		
		Receives message packet Logs transaction Decodes packet Identifies product sending packet Passes packet to Product Handler corresponding to product	
			Logs received packet Validates packet serial number If not found, returns error packet to application Else, returns packet with data/action back to application (e.g., URL)
	Receives packet If error, display error message Else, display data or perform the requested action (e.g., launch browser and link based on received URL)		
Sees the data/action associated with the object (e.g., views web page)			

The present system generalizes this example to support any product from any vendor that is capable of sending a message via the Internet that complies with the expected request format (e.g., a product code, message type, and identifier) and receiving a message in a corresponding response format. One set of message formats suitable for use in such a system are described in more detail below.

Watermark Registration – the first step in the process

In order for the system to identify the response (e.g., a URL) that corresponds to an object identifier (e.g., a watermark), this data must first be associated within the database 17 in association with the watermark to which it corresponds. The watermark registration process captures some basic identification information used later to validate the incoming message, and identifies the associated information/action. In the illustrated example the identification information includes:

- Customer Account,
- Object and associated attributes (name, description, expiration, etc.),
- Action, and
- Registered Serial Number (for registration updates)

The Customer Account identifies the watermark registrant. In most cases, this is also the party to be billed for services. For validation and security reasons, the Customer Account is required to be a known, existing account. Account information, including the account's password, is maintained by an Account Management system.

The Object and associated attributes identifies the object to be watermarked. The object attributes typically include the name and description of the object and a list of accounts authorized to access the object's registration. These authorized "supporting" accounts are typically the ad agencies, pre-press houses, etc. involved in the watermark embedding process in the print advertising example contemplated herein.

The Action defines the response the customer desires when the watermark is detected. It varies by product, but in the illustrative embodiment involves the return of some additional information regarding the watermarked object. In the illustrative system, the action is return of a URL or HTML to be used to display a web page associated with the watermarked object. For other products, the desired response may be display of the object's owner & rights information, software/data downloads, delivery of streamed audio or video, presentation of an advertisement, initiation of object-based actions, etc.

The Registered Serial Number forms the last component of the registration. It is this assigned vendor and product-unique identifier that allows the system to acquire the specific information/action for the object in question.

A few key product Registration concepts -

Watermark Registration is a product-specific process –

To allow each of the products the freedom to upgrade their capabilities without impacting any other product function or schedule, the registration process is product-specific.

Watermark registration is web-enabled -

The exemplary registration is a web-enabled process that requests the basic identifying information from the object owner (publisher, ad agency, studio, etc.) and returns to the registrant a packet with a unique identifier to be embedded within the object. A watermark embedding application (i.e., software) uses this packet to embed the watermark type and serial number within the client's object.

In the illustrative system, only one watermark may be embedded within a single object. In other embodiments, multiple watermarks may be embedded into a single object.

When a customer registers a watermark, the system associates the watermark serial number with the information provided by the customer during the registration process. The associated information may vary with different products. One set of associations, for the exemplary magazine advertisement objects, is shown in the following table:

Mandatory?	Information	Comments
Mandatory	Customer	Typically, the publisher
Mandatory	Publication(s)	Magazine(s) containing the ad
Mandatory	Issue Date	First date of the magazine/publication period
Optional	Volume	Magazine/publication volume information
Optional	Region Code	Optional information for regional publications
Optional	Location Code	Location of the object within the publication (e.g., page and, optionally, finer location data)
Mandatory	Watermark Type	Watermarks may have varying type. The type defines how to interpret the Serial Number
Mandatory	Serial Number	Assigned watermark number
Mandatory	Object Name	Customer's name for the object
Mandatory	Object Description	Customer's textual description of the object
Mandatory	Object Type	Ad or Editorial (and in other systems: Direct Mailer Card, Product Packaging, Coupon, Catalog, Business Card, Credit Card, etc.)
Optional	Campaign	For ads and promotions, the campaign name
Optional	Object size	Stated in fractions of the page (full page, half, etc.)
Mandatory	Effective Date	Date on which the user will first be able to initiate any actions. For publications, typically this is the "on stand" date
Mandatory	Expiration date	Date/time when the watermark expires
Mandatory	Primary Action	Initially the URL used for redirection
Mandatory	Primary Effective	Date the Primary action becomes effective
Mandatory	Primary Expires	Date the Primary action expires
Optional	Default Action	Reserved for future use (e.g., backup to the Primary action)
Optional	Default Effective	Date the Default action becomes effective
Optional	Default Expires	Date the Default action expires
Optional	E-mail address	Used to automatically notify the Customer of problems with the registration/Action
Mandatory	Status	Incomplete, active, inactive
Optional	Problem Indicator	Bad URL, slow site, etc.
Optional	Supporting Accounts	This field and its sub-fields are repeated for each supporting account
Optional	User Fields (4)	
Optional	Text	User Field free text
Optional	Viewable by Others?	Y/N. N hides the field form any other accounts

Table 1. Registration Database Elements

Watermark registrations expire -

For some products, watermarks are granted only for a limited period of time. For these watermarks, the Registration process employs an expiration date for the assigned serial number. When the system receives a message requesting action for a serial number that has expired, an error is returned. Registrants may extend their watermark serial number expirations by updating the expiration date. Expiration extensions may result in customer charges.

Watermark registration can be completed in one or more web sessions -

Registration can be a single or multi-step process. If the media owner has all of the required information at the start of the process, the system can provide a simple web-enabled method for requesting a watermark serial number (s) on-line. With all of the information provided, the registration is considered "active." That is, it is available for immediate use by the consumer. If the registrant does not have all of the required information available at the initial session, by providing a minimum set of information (e.g., name and/or organization name + product), a product watermark serial number may still be issued for the registrant to use in the embedding process. The most typical use of this partial registration occurs when the actions associated with the media to be watermarked (e.g., URL, etc.) are not yet known. The partially registered serial number is considered "inactive" until all of the required registration information has been completed. The system will issue an error message if requested to process an "inactive" serial number. Whether active or inactive, these registrations may be considered billable items subject to the terms and conditions of the applicable contract(s).

Registrations can be updated by the customer to reflect new information and/or to complete a previous registration session. For example, a registered customer may request a watermark serial number without specifying the URL used to redirect the consumer. The system will assign a serial number so that the customer can continue with the embedding process, but the registration will not be considered complete until the customer updates the registration with the URL and any other mandatory information regarding this serial number.

Watermark registrations are secure -

Only the registrant and those accounts that the registrant authorizes can access specific watermark registrations.

In the illustrated system, the customer account that registers a watermark may grant permission to a specific ad agency and/or pre-press house to change certain fields within the registration as a normal part of their work. Each customer, agency and pre-press house needs an account on file to be granted access to watermark registrations. The Customer account is established as part of the contract process. For ad agencies and pre-press houses, the accounts are established on an as-needed basis, through a controlled web site accessible to the customer.

For all products, the same basic tenet holds – access to the registration information is limited to only explicitly authorized accounts. Accounts are password protected. For ad agencies and pre-press houses, a single password may be shared. In other embodiments, each part may be assigned a unique password.

Watermark registration changes are logged –

All registration actions – creation, modification and deletion - are logged in an audit log. The authenticated username, the date/time of the action, and the action itself are all stored to provide a complete audit trail.

Processes and data flows associated with registration are illustrated in Fig. 6.

Entering Data into the Registration Database

While the client application, router, and product handler have initially been described in connection with responding to watermark information sensed from media objects, the same infrastructure can be employed earlier in the process, to enter data into the registration database 17. That is, a suitably configured variant of application 28c can be used by publishers, ad agencies, pre-press houses, etc., to (a) provide initial data to the database; (b) update such data; and (c) query the database for current values. Alternatively, a dedicated registration server 19 (Fig. 2) can be employed.

The involvement of plural parties in the registration process can be facilitated by encapsulating the database record contents for a given watermark in a file to which information is successively added (or updated) by different entities, and used to convey data between the database 17 and the cited entities.

Consider a case where Nike advertises in Wired magazine. The ad department at Wired agrees to sell space in response to a request from a media buyer at Nike. Wired may start the related watermark work by securing from the operator of system 10 a particular watermark identifier. (This, and most of the following procedures, are effected by computers talking to computers in accordance with instructions provided by suitable software used by the various participants, etc. In the discussion that follows, this software is the registration server 19 although, as noted, product handler 16 could be arranged to perform these functions.) Wired provides the operator an issue identifier (e.g., San Francisco edition of the July, 2000 issue), and internal tracking information used by the magazine. Registration server 19 responds by sending Wired a confirmatory file, by email, that encapsulates the information thus-far (i.e., the watermark identifier, the issue ID, and the magazine tracking information). Server 19 creates a new database record, and parses the received information into corresponding fields of the record.

Wired forwards the file received from the registration server to the media buyers at Nike. Nike supplements the information with its additional data, including the name of the advertisement and internal tracking information. It then forwards the updated file to server 19. Again, this server processes the file and updates the database record with the new information. It emails a confirmatory data file to both Nike and Wired, so each has the latest set of information.

The process continues in this fashion. Each entity provides new data to the registration server 19 via an emailed encapsulating file. The server updates the corresponding database record, and dispatches updated versions of the encapsulating file to the identified participants so each has the latest information.

Once Nike has entered its data via this process, it may forward the encapsulating file to its outside ad agency. The ad agency uses the file similarly, adding its particular information, and forwarding the file to the server. The server updates the database record accordingly, adds the ad agency

to its email distribution list for encapsulating files, and dispatches the latest version of the file to Wired, Nike, and the ad agency.

A pre-press house may be the next party involved, and so forth.

Identification of the URL to which the watermark ID corresponds, and updating of the database record accordingly, may not happen until near the end of the process.

At any time, any of the parties can provide additional information to the database, and share such information with others, via the same process. (Some information may not be suitable for distribution to all involved parties, and can be flagged accordingly.)

Server 19 needn't always be the hub through which all communication takes place. The file as updated by Nike, for example, can be forwarded by Nike directly to its ad agency. The ad agency can add its information, and then provide the twice-updated file to the server, etc.

By using distributed files as proxies for the actual database record, a number of advantages accrue. One is local availability of the latest information by all parties without the need for an internet connection. Thus, if a creative director wants to work on the beach, or otherwise disconnected from the net, the needed information is still available. Another is the ease of integrating software tools at each of the parties with a file of local data specific to a particular advertisement, rather than requiring the architectural hassles of interfacing with a remote database and navigating its attendant authentication and security hurdles.

While the foregoing discussion made reference to emailing files, a typical email program would not normally be used. Instead, to better manage the attendant logistics, a specialized file management/mail program is used by each of the parties. Such program would track the latest file for each advertisement, making same readily available for updating as desired, and index the files by various content fields. The user interface could thus present a list of files, grouped or sorted by any of the database fields, permitting editing or adding of information just by clicking on a given field or tab.

Of course, the file-distribution system just-described isn't essential to the system. A great variety of other arrangements can naturally be employed. One is for each party to log-on to server 19 as needed to inspect, or update, database fields for which it has appropriate permissions.

Numbering Schemes

The payload information encoded into objects (e.g., by watermarking) can take a number of forms and sizes. Four exemplary classes are discussed below:

a) Domain-based payload segmentation;

b) Customer/usage-based payload segmentation;

c) Unsegmented payload; and

d) Unique ID

Domain-Based Payload Segmentation

Domain-based payload segmentation approaches divide the payload into fields, each with a distinct meaning. The CLASS/DNS/UID arrangement earlier detailed is exemplary of this type of approach.

Consider a payload of 60 bits. Twelve bits may form a Class ID. These bits serve as an identifier for a top-level domain. 24 other bits may form a DNS ID. These bits identify an intermediate level domain. Together, the Class and DNS IDs fully identify the class of objects from which the data originates, the customer, and the server that should respond to the payload. (Some responses may be handled by the client computer, rather than dispatched to a remote server.)

The remaining 24 bits are a User ID, and serve as the most granular identifier, indicating the particular source of the payload. Based on this ID, the responding server knows exactly which response is to be provided.

This payload is embedded, in its entirety, into the customer's object. When sensed by the client computer, the application 28c parses (decodes) the payload into Class ID, DNS ID and User ID fields. The Class ID is used to trigger one or more of the client- or server-side programs. Once "launched" these products then use the Class ID in conjunction with the DNS ID and the User ID to complete the desired action.

One of the Class IDs may signify the object is a magazine page. Based thereon, the application 28c may direct the payload to the router/handler described above for response. Another Class ID may signify that the object is music. Again, the application may direct the payload to the same router. Or the application may direct the payload to a service maintained by a music industry consortium for response. Still another Class ID may signify that the object is a grocery package, and the payload should be routed to an on-line grocer for response. Yet another Class ID may signify that the object is a business card, and the payload should be processed locally, at the client machine. The mapping between Class IDs, and the corresponding response mechanism to which the application 28c should direct the payload, may be maintained by a database associated with the client computer's operating system (e.g., the Windows Registry), as detailed earlier.

Once the payload has been dispatched to a proper response destination, that entity examines the DNS ID to further classify the correct responding entity. For example, different IDs may correspond to different classes of servers within a tree of servers.

One the payload has been directed to the correct class of servers, the User ID defines the terminal "leaf" in the tree (e.g., a database record) that finally defines the response.

Customer/Usage-Based Payload Segmentation

A second approach again employs a segmented payload technique. In this arrangement, however, a first field defines the interpretation of the following bits (e.g., their segmentation into different fields).

Again, consider an exemplary payload of 60 bits. Twelve bits can be a Version ID. These bits indicate how the succeeding bits are to be parsed and interpreted, and may indicate (like the Class ID in the foregoing approach) the particular application program 28c that should be used. The Version ID bits thus serve to indicate the payload type. In the illustrated embodiment, one of these types signifies that the payload is coming from a magazine page and should be handled accordingly. In this case, the remaining 48 bits can be parsed into three fields: Owner ID (15 bits), Publication ID (15 bits), and Media ID (18 bits).

The Owner ID identifies the customer to whom the watermark is registered (e.g., Nike). This is used for ad effectiveness analysis and billing purposes. The Publication ID identifies the particular publication (e.g., July, 2000, San Francisco edition of Wired Magazine). The Media ID identifies a particular page location within that publication.

As before, the payload is embedded in its entirety into the customer's object. The payload is first parsed to determine the Version ID. If the user's device 12 has been programmed to handle such objects locally, further parsing is performed in accordance with data corresponding to that Version ID, and associated processing of the parsed data is performed. If the device has been instructed to dispatch such payloads to remote locations for service, the complete payload can be dispatched with only such further parsing (if any) as may be required to correctly identify the corresponding remote servicing entity.

Unsegmented Payload

An unsegmented payload consists only of two parts: a Version ID (as described above) and an Object ID. In an illustrative case, a 60-bit payload is again used, with 12 bits serving as the Version ID, and the remaining 48 serving as the Object ID.

In this approach the relationships of owner/customer, publication, issue, and media are all maintained in database 17 rather than literally represented in some fashion within the object identifier.

Unique ID

This case is akin to the unsegmented payload, but consists of just a single field – a unique identifier. The same application 28c is always used, and always treats the payload data consistently (e.g., processing locally, or dispatching to a predetermined destination) regardless of the payload contents.

Combinations and hybrids of the foregoing approaches can of course be used. Moreover, the 60 bit payload length is illustrative only. Longer (e.g., up to 1024 bits) or shorter (e.g., down to 8 bits) payloads can naturally be used.

In a particular embodiment, a 32-bit unsegmented payload is used, consisting of 10 bits of payload type and 22 bits of watermark serial number. Some materials (e.g., advertisements including composite graphics) may be encoded with several serial numbers. The mapping between this payload and the customer/publication/etc., is maintained in database 17.

(As noted below, the data sent from the application 28c typically includes information other than the identifier payload, e.g., the type and version number of the application 28c, the electronic address of the dispatching application, etc.)

Router

The router 14 permits any number of different products to be used by the indicia detection and response model. By keeping this function separate and generalized, new products can be added without design changes to the existing products or the product handlers 16. There are two keys to making this approach successful – speed and flexibility. By using a standardized, open interface, the router is able to facilitate both of these goals.

A premise of an exemplary interface is an enveloping technique that allows the router to "open" the outer transaction envelope and extract the vendor and application ID without decoding the remainder of the transaction (message). Given these two pieces of information, the router uses a simple lookup table to determine the product handler appropriate to complete the transaction. The router then passes the vendor, application, remainder of the transaction and the Internet "reply to" address on to the appropriate product handler. The simplicity of this handling keeps the routing delay to a minimum, while deferring the actual response processing to vendor/product-specific handlers. By including the "reply to" address in the data passed on to the product handlers, the router is freed from the responsibility of return routing for the product's response(s).

To review, the router:

1. decodes the request packet received from the client products into the packet's base components – Vendor ID, Application ID and message;

2. validates the request packet base components against a list of known, good values;

3. if a request packet component is found to be invalid, issues an error message noting the invalid components and returning same to the calling session (e.g., product);

4. sends the decoded request packet contents and any required identification of the calling session to the appropriate product handler; and

5. reports any errors encountered, including invalid packets received, to a system monitor.

Certain data flows associated with the router are shown in Fig. 5.

Product Handler

The primary function of the illustrative product handler 16 is to process requests received from the application 28c, via the Internet and router 14, and return the requested information/action to the originating device 12. In the illustrated embodiment, the information requested is the URL associated with the watermark payload sent by the application. In other embodiments, other actions and/or information may be requested.

Each received watermark payload is validated using information in the database 17. If the watermark payload ID is found and is active, the requested action is performed. If the watermark payload ID is not found or is in an inactive state, an error message is returned to the requesting application.

All requests are logged in a transaction log for tracking and billing purposes. This includes any secondary payload information (zip code, Demographic Household ID, etc.) passed in by the application 28c. The log can be maintained by the product handler 16, or elsewhere.

To speed system response, the product handler 16 may anticipatorily send URLs to the application corresponding to watermark payloads the handler foresees may be coming. These URLs can be cached in memory associated with the application 28c, and quickly recalled if needed by the application.

Consider, for example, a magazine containing watermarked advertising. If the user presents a first ad to the device 12, the watermark is decoded and forwarded to the product handler 16, which responds with a URL corresponding to that ad. The application 28c then passes that received URL to a web browser 28b on the device 12, which initiates a link to that internet address. But the handler now knows the magazine the user is reading. By reference to the watermark first received, the handler may discern, for example, that the user is reading the San Francisco edition of the March 14, 2000, Time magazine, and just looked at page 85. Based on this information the handler can query the database 17 for URLs associated with other advertising in that issue. (The database index is structured to permit fast queries identifying all ads in a given magazine issue or other collective data source.) These URLs are passed back to the application 28c and cached. If the user next presents an advertisement from page 110 to device 12, the application 28c finds it already has the corresponding URL locally cached. The application then passes the corresponding URL to the web browser. The web browser initiates the link immediately, obviating a data round trip between the application and the remote system.

The caching can be optimized in a variety of ways. One is to first send URLs corresponding to pages that are next-expected to be encountered. For example, if the user just presented page 85 to the sensor 22, after sending the URL for that page, the handler 16 would next send the URLs associated with pages 86, 87, etc. On sending the URL for the last page of the magazine (typically the rear cover), the handler could start from the beginning (typically the front cover) and send further URLs up to that for page 84. Another optimization is to first cache URLs for the most conspicuous ads, e.g., first send URLs for any 2-page spread ads, then for each full page add, then for each successively smaller fractional-page ad. Still another approach is for handler 16 to dispatch URLs to device 12 for caching in accordance with a contractually-agreed priority. One advertiser, for example, may pay a premium ad rate in exchanged for being cached before other advertisers who don't pay the premium. Other caching priorities, and combinations of such priorities, can naturally be employed.

In some systems, the advertisers or publishers may be charged for use of the system based on the number of URLs served by the system for linking. If local caching of URLs (e.g., at device 12) is employed, it is desirable for device 12 to report to router 14 (or handler 16) the URLs that are actually retrieved from the local cache and used for linking, so that the remote system can log same. Thus, each

time the user presents an object to sensor 22 for which a corresponding URL is already cached, application 28c dispatches a message to router 14 reporting the event (and, usually, the particular URL involved). This event is then logged in the transaction log.

This anticipatory dispatching of URLs is one alternative function that may be performed by a product handler. Another is if the application 28c queries the product handler to determine if a more recent version of the application is available for download. If so, the application – through interaction with the user – can request that the product handler respond with a software download.

In greater detail, application 28c can periodically query the product handler as to the identity of the latest version of application 28c (e.g., the first time the application is used each day). Device 12 may have version 3.04, and the remote system may respond that version 3.07 is the most current. In such case the application 28c can alert the user – by suitable text, graphics, or other means – that a more recent version of the program is available, and query whether such updated version should be obtained. If the user so-instructs, handler 16 can serve to device 12 the latest version of the application (or a patch permitting the presently-installed version to be updated).

Sometimes it may not be necessary to update the application version. Instead, data from the remote system may indicate the desirability, or necessity, or changing just one or more parameters in the application 28c. For example, new security keys can be dispatched periodically by handler 16 to device 12, and used to change the security configuration of the application. Or the application 28c can be instructed to direct further outgoing watermark traffic – either for the next hour, day, or until instructed otherwise - to a different router 14. Such instruction can be used to optimize system performance, e.g., for router load balancing purposes, to avoid internet routes that are found to be slow, etc.

In summary, the detailed handler:

1. validates the received identifier (e.g., watermark serial number) against the list of active identifiers; and, if the serial number is not found, return an error message to the calling session, and log the error to an error handling routine;

2. for each received, valid watermark serial number, finds the corresponding active primary action from the database;

3. for each received, valid watermark serial number, if the handler finds the corresponding primary action is currently not active, it performs an alternative, "default" action instead;

4. if the handler finds an active primary action associated with the received valid watermark serial number, it returns the URL for application use in redirection (round trip approach), or serves the HTML page found to the calling session;

5. if the handler does not find an active primary action associated with the received valid watermark serial number, but does find an associated default action, it returns that URL for application use in redirection (round trip approach), or serves the HTML page found to the calling session;

6. if the handler does not find a valid, active primary or default action associated with the watermark serial number, it returns an error message to the calling session, and logs the error to the error handling routine;

7. records each transaction, including those that result in error messages, for billing and analysis purposes (in other embodiments, this function may be performed by the router, instead);

8. responds to a "software version request" by returning the most recent available application software version number to the calling session;

9. responds to a "software download request" by initiating a file transfer of the most recent available application software to the calling session;

10. responds to a valid Request for Registration packet upload (proper format, an existing serial number, an account ID and a valid corresponding account password) by returning a current registration packet for the provided watermark serial number;

11. responds to an invalid Request for Registration packet by returning an error message to the calling session noting the failure;

12. responds to a local transaction cache flush request by writing the locally cached transactions to the transaction log; and

13. responds to a multiple URL request by returning the URL associated with the provided serial number first, followed by all other active serial numbers and URLs for the publication, issue and region code (optional) provided.

Certain of the above-described processes associated with the product handler are shown in Fig. 6.

URL Performance Monitoring

Returning to operation of the system, the URLs identified in database 17 may, from time to time, become inoperative or impaired due to equipment problems at the remote web site or otherwise. If desired, the handler 16 (or another component of the system) can be programmed to periodically test each of the links registered as active in the database (e.g., once per day), and measure the time for the associated web page to load. If the web page doesn't load, or takes much longer to load than usual (and re-tests confirm that the condition isn't an anomaly), those conditions can be flagged in the corresponding database record. If the handler is requested to provide such a URL to a device 12, the handler can send a message – either with or without the URL – indicating to the device that the URL is misbehaving.

If the URL is working, but is unduly slow to load (either compared to its historical performance, or compared to other URLs), handler 16 can provide an interim diversion to the device 12. For example, it can instruct the device to launch a second browser window, and direct that browser to an alternate destination to entertain the user while waiting for the intended page to load. When the intended page is finally loaded, the first browser window can be displayed - either by closing the second, diversionary window, or by bringing the first window to the front while keeping the second window alive in the background.

This alternate destination is desirably a low bandwidth page, so that it will not unacceptably further slow loading of the desired URL. This alternate page can be one selected by the handler, for

which the URL is sent after the desired URL. Or instead of providing a URL from the handler, the handler can serve an HTML or other page directly to the device 12. Or the alternative URL can be stored at device 12 and used to invoke the second browser window upon receipt of data from handler 16 indicating that the desired content will be slow in coming. In some embodiments the user can identify several alternate URLs (e.g., weather, stock info, jokes) and the handler or the application 28c may select among them randomly or otherwise. Or an HTML page or other application can be loaded locally at the device 12 in response to a "get ready to wait" indication from the handler 16.

If a URL is marked in the database 17 as slow or inoperative, the scanning operation periodically rechecks the URL to see if its status in the database should be changed (e.g., changed from inactive to active). Inactive URLs are reported to the registrant by email, and flagged for manual follow-up if not restored to action within a predetermined period.

Illustrative Responses by Product Handler

Part I, above, provided a sampling of the great variety of diverse applications enabled by the illustrated system 10. A few more are detailed below.

Consider use of the system 10 to enable personalized greeting cards. A greeting card company may prepare watermarked press-on stickers for use with its cards or other correspondence. The customer shows the sticker to a camera-equipped computer (either at the retail store, at home, or elsewhere). The computer decodes the watermark and sends same to a corresponding product handler 16 through the router 14. The handler – recognizing the watermark as an unregistered greeting card sticker – invites the customer to enter a destination URL, such as the customer's personal web page. This information is entered by the consumer and forwarded to the remote system for entry in the registration database 17. Thereafter, whenever the sticker is shown to a suitably-enabled system (e.g., by the card recipient), a browser window is automatically launched and directed to the web page specified by the purchasing consumer. (The same result can, of course, be effected without use of stickers, e.g., by encoding the greeting cards themselves.)

In some applications, the product handler may have a library of different responses it can provide to a user in a particular context, depending on the user's further selection. Consider a university student having a suitably-watermarked university ID card. When the card is presented to a device 12, the product handler replies with HTML instructions causing an options menu to appear on the device screen, e.g:

1. Review calendar of upcoming university academic events
2. Review calendar of upcoming university sporting events
3. Review present class schedule
4. Select courses for next semester
5. Review grades

When the student makes a selection (e.g., with a mouse, or by moving the ID card in a specified manner), the application 28c dispatches data corresponding to the selected option to the product handler, which then responds with the requested data.

In some cases (e.g., Review present class schedule, Select courses for next semester, Review grades), care must be taken to protect such information from persons attempting access using lost or stolen IDs. Accordingly, when any of these options is selected, the handler 16 may first respond to device 12 by querying for a password or PIN. Only after entry of the correct password/PIN is the requested action performed. (For security reasons, the university may prefer that the password authentication process be performed by a dedicated on-campus server, rather than by product handler 16. Naturally, this and other tasks can be delegated to processors other than handler 16 as best fits the situation.)

In other cases, an option menu needn't be presented – the correct response is inferred from the context or environment. Consider a drivers' license that is watermarked with identification of the owner. If presented to an email kiosk 12 at an airport, the decoded watermark may be used to look-up an email account corresponding to that individual, and download new mail. If the same drivers license is presented to a check-in kiosk, the decoded watermark may be used to look up that person's flight reservation and issue a seat assignment. In both cases the kiosks can be essentially identical. One, however, identifies itself to the router/product handler as an email kiosk, the other as a check-in kiosk. The response undertaken by the router/product handler differs accordingly.

Returning to the university example, there may be cases in which students are tempted to swap photos on a student ID, e.g., to permit an imposter to take a graduate school qualifying exam on behalf of a less-qualified student. In the usual case, such photo-swapping may be difficult to detect. This problem can be combated by an exam check-in procedure that includes having each student present their ID to a device 12. An application 28c specialized for this task can forward a watermark decoded from the ID photograph to a handler 16, which responds by causing an image of the identified student to be displayed on device 12. (The university could compile the requisite database of student images as it issues ID cards.) If the exam proctor sees an image on the device that does not match the image on the ID card, appropriate action may be taken. (This arrangement is applicable wherever photo ID documents are used, including airport check-in, customs, immigration, etc.)

Still another application of the illustrated system is to look-up, or act on, meta-data associated with a marked object. Consider an image, video, or audio file that a user downloads from the internet. Familiar applications such as Microsoft's Windows Explorer (including Internet Explorer) may be configured with watermark decoders activated, e.g., from a Properties panel (accessed, e.g., by right-clicking on the file icon or name and selecting the "Properties" option). When a watermark is detected in a file, the Explorer application can send a corresponding packet to a remote system (e.g., the depicted router/product handler/database). The remote system recognizes the packet as originating through the Properties panel of Windows Explorer, and looks-up the watermark ID in a database 17. Meta-data corresponding to the file (e.g., proprietor, creation date, licensing terms, exposure data, subject, etc.) is

returned from database 17 (or from another database identified by the router, handler, or database) to the application 28c, and is displayed in the Properties panel (optionally under an appropriate "tab").

(The present assignee has long offered a "MarcCentre" service that serves as a clearinghouse through which watermark identifiers found in photographs, etc., can be used to identify the proprietors and associated information corresponding to such objects.) In embodiments of the present utilizing this service, the router 14 passes the request to MarcCentre server (a product handler in this instance), which provides the solicited information back to the originating application. The present assignee's MarcSpider service complements the service provided by the Media Commerce product. The MarcSpider service constantly scans Internet sites evaluating each graphic encountered to determine whether it contains a watermark. (Audio and video can be similarly analyzed.) With each detected watermark, the MarcSpider service records the graphic file name, size, format, date/time and URL where the graphic was found. This information is then made available to MarcSpider customers in report form.)

Instead of simply displaying the meta-data, the application and/or the remote system can make use of it. For example, if the meta-data indicates that the proprietor of a watermarked image is Corbis, and that the image can be licensed for a certain use under certain terms, the remote system can be utilized as a licensing server – receiving payment information from the user, granting the license, and forwarding transaction details to Corbis.

Still another application is the sale or promotion of music or video over the internet. Taking the case of music, an artist may freely distribute a low-fidelity (or otherwise corrupted or abridged) version of a song. The low fidelity can be by reason of bandwidth limitation (e.g., 500Hz – 2.5 KHz), monophonic (as opposed to stereo), or otherwise. The artist can seek to distribute the low-fidelity version as widely as possible, to serve as a marketing agent for the artist's other works. (The free distribution of lower-bandwidth audio may serve to alleviate some of the network bandwidth problems faced by universities whose students actively engage in transferring free music over the internet.)

Each low-fidelity version can be processed to extract an identifier (e.g., a steganographic in-band watermark; a numeric ID or song/artist name field in a in a file header; a 128-bit hash value obtained by applying a hashing algorithm to the music data, the music file header data, a portion thereof, etc.) If a listener is interested in obtaining a full-fidelity version of the work, the listener can operate a suitably programmed computer or music appliance that extracts the identifier from the work and passes it on to the remote system. The remote system can respond in various ways, e.g., by providing a full-fidelity version of the same work back to the user (such as MP3 download) and charge the user's credit card a fee (e.g., $0.99); or by directing a web browser on the user's computer to an e-commerce/fan web site associated with the music, etc. Such functionality can be provided in general purpose programs such as Microsoft's Internet Explorer, e.g., by right-clicking on a file to obtain a menu that includes this and related functions.

Figs. 8-10 show a sequence of screen shots from such an embodiment. In Fig. 8, a user has right-clicked on an MP3 file icon in a directory listing 200. A property menu 202 pops up that includes, as its second option "MP3Bridge."

Fig. 9 shows what happens when the user selects the MP3Bridge option. An MP3 player 204 is launched, and a dialog box 206 appears. The dialog box queries the user, "More Information About the Artist? Yes No."

Fig. 10 shows what happens if the user selects "Yes." The software sends the identifier – extracted from the MP3 file – to the remote system. The remote system responds with the address of an associated web page, and instructs the user's computer to launch a new browser window directed to that page.

The same functionality can naturally be invoked through the user interface of the MP3 player (or a Windows MediaPlayer, etc., rather than through Internet Explorer). The music application can spawn a separate window, or present the options and the associated data within the existing window.

Yet another application of the remote system is as a "net nanny" filter. Links requested through the system can be checked for keywords, adult-content flags, content ratings, or other indicia of age-suitability, and provided to the requesting computer 10 only if they meet certain earlier selected criteria.

Again, it will be appreciated that the foregoing examples are but a few of myriad applications enabled by the detailed system.

Reporting

System software may enable the provision of customer-accessible reports (accessible over the internet) that show detailed and summary usage information by date, customer, publication, issue date, region, product/version, etc. These reports can be both regularly scheduled and ad-hoc. The specification of the content, relationships and the timing of the reports can be defined by the customer on-line.

Illustrative reports detail:

a) Hit rates/Transactions per customer per ad
b) Hit rates/Transactions per customer per publication per ad
c) Hit rates/Transactions per customer per publication per issue per ad
d) Hit rates/Transactions per customer per publication per issue per region per ad
e) Hit rates/Transactions rates by originating application (28c)
f) Hit rates/Transactions by originating application vendor
g) Hit rates/Transactions rates by originating web domain (e.g., aol.com)
h) Hit rates/Transactions rates by postal/zip codes
i) Hit rates/Transactions by country

Additional marketing/marketplace reporting can also be produced for internal analysis by the service provider, and for sale to other entities. These reports typically provide a more global view of the impact and usage of the system. Using information stored in a demographic database, in conjunction with these usage patterns, the system can provide customers and research agencies with more detailed demographic/statistical data on the system's usage and effectiveness.

In an illustrative system, certain statistics in the demographic database are compiled using statistics from a sample of users that consent to have their activities tracked in some detail, in

consideration for certain perks (e.g., give-away cameras, bar-code scanning pens, or other devices, etc.). These users are termed Demographic Households. A software program included in the systems solicits information detailed in the following table from such users over the internet, with a web-enabled interface. A related program allows such users to update/edit their user/household information previously entered. Each such session is password authenticated for security.

User Information	Comments
Name	
Address	
Street	
City	
State	
Country	
Postal Code	
Phone number	
E-mail address	
Household Annual Income	Provided as raw $ or as a selection from a range of numbers
Occupation	
Education	May be per member of household.
Profession	If applicable
Number of members of household	
Member of household	
Age	
Sex	
Internet user?	
User of this linking service?	
Internet usage per week	In hours. Sum of entire household
Internet business usage per week	
Primary Internet usage?	Typical household use of the Internet. May be a selection list
Owned a computer since?	Year only
Number of computers in the home?	
Types of computers in the home?	Mac, PC, etc. Select all that apply
Rooms where the computers are located	Home office, bedroom, etc. Select all that apply
What ISP do you use?	
What is your modem speed?	Select from list that includes ISDN, ADSL, cable + dial up modems.
Are you willing to be an official "Demographic Household" and allow us to contact you for feedback on our products and advice on new products?	
What other technology devices do you have in your household?	Scanners, PC cameras, digital cameras, DVD, PDAs, etc. Select all that apply

Audio and Video

As with paper advertisements, the illustrated system provides users of web-connected PCs or other appliances with methods of obtaining information, content, associated products, or associated services using the same principles as detailed above.

For example, an application 28 can "capture" music or other audio using a recording device (note recorder, microphone connected to PC, MP3 player, etc.) and analyze the captured audio to detect an embedded watermark. Once detected, the application passes some or all of the watermark payload information, together with identification of the application and its vendor, to the router. The router forwards the payload information to a handler corresponding to the application. The response of the product handler varies with the context and nature of the data. For example, the handler may return the artist, title, track, album, web URL and purchasing information, to the user. Recorded news and entertainment segments may include transcripts (audio, video and/or text) of the segment along with other related web site information. The handler may simply cause the device 12 to launch a browser window directed to a music commerce web site where the music can be purchased.

Security

The system's basic security philosophy is to grant access to each customer's information only to the users authorized by the customer. To this end, the system desirably should:

1. Create and maintain a list of authorized users (accounts).
2. Employ security methods to deny access to any unauthorized users.
3. Limit users to access only the objects they are authorized to access (typically, the objects belonging to that customer).
4. Report and record all unauthorized access attempts.
5. Maintain a log of all authorized user logins (sessions).
6. Provide the capability for the watermark registrant to grant access rights to other accounts (such as ad agencies and pre-press houses).
7. Establish initial passwords for each account
8. Provide the capability for each authenticated user/account to change their password
9. Provide the capability to reset an authenticated user/account's password in the event the current password is lost.
10. Store all passwords as encrypted values (to prevent theft of passwords).
11. Provide the capability to restrict the creation, modification, deletion, and listing/viewing of account information to authorized users.

Audit Trail

Because of the financial implications of the system's activities, all changes to any registration or customer data need to be recorded. This audit trail provides the operator and its customers with an accurate accounting for the current and previous states of the data.

The audit software desirably records the creation, modification, and deletion of all registration and customer data. The audit software also records the username, date/time of creation/modification/deletion of records, and – for modifications – the before and after images of the data changed.

Application-to-Product Handler Interface Definition

The basics of the interface between the application 28c and the handler 16 are (a) a flexible request and response package structure, and (b) a defined connection method based on industry standards. The illustrated messaging employs the http and/or the https protocol to send and receive messages among the system components. An overview is provided in Fig. 4.

Message Format

The message format is XML-compliant and is defined by the following XML DTD –

```
<!DOCTYPE list [
<!ELEMENT Content (vendor, appl, prod)>
<!ELEMENT vendor (#PCDATA)>
<!ELEMENT appl (#PCDATA)>
<!ELEMENT prod (#PCDATA)>
]>
```

The application 28c appends its data to this header for transmission to the product handler 16. Exemplary messages and product handler responses are detailed in the sections that follow.

Application Message Definitions

The application message definitions can be broken down into Request Code, Primary and Secondary information.

The **Request Code** instructs the product handler 16 to take a specified action.

The **Primary information** portion contains the data required to properly service the application's request. The Primary Information varies based on the Request Code.

The **Secondary Information** is intended for use by analysis and reporting tools and does not instruct nor aid the product handler in servicing the user's request. Secondary Information contents change based on the Request Code and not all Request Codes are required to have associated Secondary Information. In addition, most of the Secondary Information requires the consumer to grant express consent to its collection. If that consent is not given, the application does not send Secondary Information. A special case exists for selected, consenting consumers to become part of a demographic database.

Primary and Secondary information may change by request type, but in general conform to the definitions below. The generic format for the product handler is also defined below.

Primary Information includes the Application Version, Watermark Type, Watermark Serial Number, Context and Environment.

- Application Version: used by the product handler to modify its actions, typically for backwards compatibility
- Watermark Type: top 9 bits of the illustrative watermark payload. Used by the product handler in processing the Watermark Serial Number
- Watermark Serial Number: remainder of the watermark payload. Provides the index used by the product handler to access the watermark in the registration database
- Context: instructs the product handler to modify/refine its action based on the consumer request's context
- Environment: instructs the product handler to modify/refine its action based on the consumer request's environment. (The environment may be specified, e.g., as home, office, car, portable appliance, etc.)

Other Request codes can, of course, be used. Each may have its own list of mandatory and optional Primary Information fields. Optional fields are excluded from the primary Information when there is no value associated.

Secondary Information:

- Demographic Household ID: identifier for a selected demographic group. This is used as an index to the actual demographic
- Input device: Manufacturer, model and version of the device used to detect the watermark (e.g., a TWAIN driver string)
- Operating System: operating system in use on the consumer PC
- Processor: processor type/class on the consumer PC
- Processor speed: processor clock speed, in MHz, of the consumer PC. (May be entered by user, or auto-detected.)
- Language: preferred consumer spoken language
- Country: Country where the consumer PC resides
- Postal Code: Consumer's postal code (used along with the country to pinpoint the location of the consumer).

(In addition to these explicit data, the packet sent from the device 12 also conveys an IP address (inherent in the use of http protocols) so that the remote device (e.g., the router/handler) has an address to which it can respond.)

Response from Product Handler

```
RtnCode            - Success =1
```

```
URL             - the active URL for the watermark serial
                number received
                      or
RtnCode         - Error <0
Error Message   - text.
```

Request for URL

Required Inputs

Header (XML format)

```
Vendor      (e.g., = Digimarc)
Appl        (e.g., = MB)
```

Data

Required information –

```
Req         =RFU
Ver         = application version number
Type        = watermark type number
Ser         = watermark serial number
Cxt         = context
Env         = environment
```

Optional Information –

```
Ctry        =User's Country name
Lang        =User's preferred Language
HHID        =Demographic Household Identifier
Det         = TWAIN string of the sensing/detecting device
OS          =User PC Operating System string
Proc        =User PC processor type and class
Speed       =User processor speed
Zip         =User postal code
```

Example:

```
<?xml version="1.0"?>
<Content>
<vendor>Digimarc</vendor>
<appl>MB</appl>
</Content>
Req=RFU
Type=1
Ser=10001
Ver=1.0
Cxt=A
Env=Q
Ctry=USA
Lang=English
HHID=1234567
Det=TWAIN string
OS=Win98
Proc=Pentium III
Speed=500
zip=74008-1234
```

Response from Product Handler

```
RtnCode=Success/Error number (Success = 1)
URL=URL associated with specified watermark type and Serial
number
Exp=Expiration date/time (GMT) for caching purposes - format of
mm/dd/yyyy hh:mm:ss
      or
RtnCode=Success/Error number (Error <0)
MsgText=message text
```

Error reasons:

-1 Type and Serial Number OK, but no URL in database (both the primary and default URL are missing)

-2 Type and Serial Number OK, but URL is marked as inactive (neither the primary nor the default is active)

-3 No record in database matching the Type and Serial Number

-4 Request format error – incomplete data

Request for Configuration

Required Inputs

Header (XML format)

```
Vendor      (e.g., = Digimarc)
Appl        (e.g., = MB)
```

Data

Required information –

```
Req         =RFC
OS          =User PC Operating System
```

Example:

```
<?xml version="1.0"?>
<Content>
<vendor>Digimarc</vendor>
<appl>MB</appl>
</Content>
Req=RFC
OS=Win98
```

Response from product handler

```
RtnCode= Success/Error number (Success = 1)
Ver=Latest Application version# available for download
https=yes (or n )
GCURL=URL used to route subsequent Application requests
      or
RtnCode= Success/Error number (Error <0)
MsgText=message text
```

Error reasons:

-5 Unknown Operating System

-4 Request format error – incomplete data

Request for Associated URLs

Required Inputs

Header (XML format)

```
Vendor      = Digimarc
Appl        = MB
```

Data

Required information –

```
Req         =RFA
Ver         =application version number
Type        =watermark type number
Ser         =watermark serial number
Cxt         =context
Env         =environment
```

Example:

```
<?xml version="1.0"?>
<Content>
<vendor>Digimarc</vendor>
<appl>MB</appl>
</Content>
Req=RFA
Type=1
Ser=10001
Ver=1.0
```

Response from product handler

```
RtnCode= Success/Error number (Success = 1)
Ser1=watermark serial number
Type1=watermark type number
URL1= URL associated with specified watermark type and Serial
number
Exp1=Expiration date/time (GMT)
Ser2=watermark serial number
Type2=watermark type number
URL2= URL associated with specified watermark type and Serial
number
Exp2=Expiration date/time (GMT)
…..
Ser'n'=watermark serial number
Type'n'=watermark type number
URL'n'= URL associated with specified watermark type and Serial
number
Exp'n'=Expiration date/time (GMT)
      or
RtnCode=Success/Error number (Error <0)
MsgText=message text
```

Error reasons:

-8 Type and Serial Number OK, but no associated watermarks or URLs in database

-9 Type and Serial Number OK, but all associated URLs are marked as inactive

-3 No record in database matching the Type and Serial Number

-4 Request format error – incomplete data

Request for Transaction Download

(Needed to account for locally cached redirections. One request per local redirection.)

Required Inputs

Header (XML format)

```
Vendor      = Digimarc
Appl        = MB
```

Data

Required information –

```
Req         =RFT
Ver         =application version number
Type        =watermark type number
Ser         =watermark serial number
Cxt         =context
Env         =environment
```

Optional Information

```
Ctry        =User's Country name
Lang        =User's preferred Language
HHID        =Demographic Household Identifier
Det         =TWAIN string of the sensor device
OS          =User PC Operating System string
Proc        =User PC processor type and class
Speed       =User processor speed
Zip         =User postal code
```

Example:

```
<?xml version="1.0"?>
<Content>
<vendor>Digimarc</vendor>
<appl>MB</appl>
</Content>
Req=RFT
Type=1
Ser=10001
Ver=1.0
Cxt=A
Env=Q
Ctry=USA
Lang=English
```

```
HHID=1234567
Det=TWAIN string
OS=Win98
Proc=Pentium III
Speed=500
zip=74008-1234
```

Response from product handler

```
RtnCode=Success/Error number (Success = 1)
                Or
RtnCode=Success/Error number (Error <0)
MsgText=message text
```

Error reasons:

-4 Request format error – incomplete data

To provide the fastest possible system response, it is desirable that data exchanges between the originating device 12 and the remote system be as short as possible – preferably of a size that can be transported in a single internet data packet (i.e., less than about 536 bits). Such an arrangement avoids the overhead associated with data division on transmission, and data reassembly on reception.

Generally speaking, the combined elapsed time of the system service (i.e., watermark recognition by application 28c, packet delivery to router, decoding by router, handling by product handler, and return of response to application) for a single request should average no more than 3 seconds as measured from receipt of request to 1st byte sent in response to request. Typical speeds are less than 2 seconds, with many responses being provided in less than 1 second.

The immediately following discussion reviews much of the foregoing, but from a different priority case and with additional details.

The MediaBridge digital message is composed of two codes, both of which are embedded in MediaBridge-enhanced images. The media *owner code* is assigned by the system administrator (e.g., Digimarc) and identifies the entity licensed to add MediaBridge enhancement to images. The *routing code* is assigned by the media owner (advertisers, publishers, manufacturers, etc.) and determines where the end-user will be directed when the Client Application reads the MediaBridge codes. Two different advertisements embedded with the same codes can take the end-user to the same web page, while the same advertisement in different publications using different codes can go to different web pages and can be used to track which advertisement or magazine is most effective in bringing end-users to the media owner's web site.

There are three major components of the MediaBridge system. The Client Application is used in homes and businesses by consumers (the MediaBridge end-users) to automatically navigate from an image or object to additional information, usually on the Internet. The MediaBridge Router provides the Client Application with the appropriate Internet address for a given image or object. The Embedding System is used by the media owners to embed the MediaBridge codes into images prior to printing.

MediaBridge Client Application

The Client Application can be distributed via OEM relationships with tethered digital camera manufacturers such as Logitech, 3Com, Creative Labs and others. It is installed by the end-user along with the camera driver and supporting software from the camera manufacturer's installation CD.

The MediaBridge Client Application may run on 200 MHz or faster Pentium or PowerPC computers configured with a tethered video camera under the Windows 95/98/NT 4.0 and Macintosh OS 8.6 operating systems.

The MediaBridge Client Application is initially focused on using MediaBridge-enhanced images to directly browse to additional information on Internet web sites. Therefore, it requires a connection to the Internet, either through a dial-up modem or a permanent connection. However, the Client Application desirably has an extensible architecture that also supports browsing to local data, e.g. on a CD, and linking to other applications.

The MediaBridge system can be used almost anywhere that a video camera can show clear, focused, high-quality images. It operates under lighting conditions varying from dim (about 40 lux) to bright (3900 lux). In very dim light it works with the aid of a supplemental light source, and in bright glare it works if the pictures or objects are shielded from the light source.

Operating the End-user Client Application

The first time the Client Application runs it desirably presents the user with a wizard that teaches the best techniques for presenting MediaBridge-enabled images to the Client Application through the video camera. The wizard is tuned for each camera and can use either the sample images or live production images.

Shipped on the installation disk (e.g., CD) can be one or more games that teach users how to best use the Client Application – e.g., focusing the camera, positioning the encoded object in the camera's focal region, holding the object stationary for the second or so needed for decoding, permissible lighting requirements, etc. The camera box, or inserts inside the box, can be MediaBridge encoded and can link through the browser to a corresponding introductory page hosted by the camera vendor or the system administrator. T-shirts or other prizes may be awarded through the web site, either on a random basis, or upon the showing of proficiency in some aspect of MediaBridge operation.

In an illustrative configuration, the MediaBridge Client Application is always running and is either active or inactive. When active, the MediaBridge video camera window is always on top of any other windows and fully visible, and the Client Application is constantly checking the video for a MediaBridge-enhanced image. When a MediaBridge-enhanced image is found, the appropriate information is displayed - most often as a web page - and the Client Application optionally becomes inactive. When the Client Application is inactive, it hides the video window, releases the camera so it is available for other applications, and uses very little memory or computer resources.

In one implementation, the Client treats the camera as a serially re-usable device. That is, when the Client Application is active and checking the video, no other application can access the video camera. Similarly, the Client Application cannot access the video when another application is using the camera.

The MediaBridge Client Application may include the following functionality:

1) **Browser/Application Launch**. When a MediaBridge-enhanced image is found, the Client launches the user's web browser or another application. When browsing to an Internet web site, the Client provides the site with the identity of the image and the end-user's zip code, if available. This information allows the media owner's web site to display a localized web page to the user. When launching another application, the Client provides the image owner code and the routing code to the application.

2) **Destination menu**. If multiple URLs are specified for a routing code, the Client Application displays a browser-based menu that allows the end-user to chose what page to display, rather than directly navigating to a web page.

3) **Branding**. While retrieving the information for displaying a web page, the Client Application displays a local web page that with a pre-stored brand (e.g., Digimarc) and explains that the desired information is being retrieved. This branding page is replaced with the media owner's page without causing any delay to the user. (The contents of the branding page may be updated during Automatic Software Update.)

4) **Flexible activation**. When the Client Application is inactive, the user can activate it by:
   a) Clicking on the application icon.
   b) Pressing a hot-key combination.
   c) Clicking on a tray icon. (Windows.)
   d) Clicking a button on the browser toolbar.
   e) Restoring the minimized MediaBridge Client video camera window. (Windows.)

5) **Status display**. While active, the Client Application provides feedback to the user through the status display pane, which is displayed in the video camera window, next to the view as seen from the camera. The status includes feedback on the ambient lighting conditions, the distance from the camera (if available,) focus, and the current state (preparing to display the image-related information, trying to read the image, or waiting for a MediaBridge-enhanced image to be presented to the camera.)

6) **Multiple camera support**. An illustrative MediaBridge Client Application uses one camera at a time, but can use any MediaBridge-enabled camera installed. If a computer only has one camera, that camera is automatically selected. If more than one camera, the user can select which camera will be used and can change the selection while the Client is running.

7) **Automatic Software Update**. The user can automatically install updates to the Client Application by making a simple menu choice. The Client connects to the Internet, and downloads and installs any available updates. In addition, the Client will suggest checking for updates if it finds a

MediaBridge-enhanced image that uses a newer protocol (e.g., by reference to a version indicia encoded with the MediaBridge data).

8) **User option configuration**. Nearly everything in the Client Application can be configured by the user.

a) Automatically starting the Client whenever the computer starts. (Default.)

b) Activation by hot key.

c) The display of an activation icon on the system tray. (Windows.)

d) Adding a button to the Internet web browser. (Internet Explorer 4 or later, and Netscape 4 or later.)

e) Selection of the last camera used on startup when multiple cameras are installed.

f) Reminder to check for software updates periodically.

g) Running the Wizard at startup. (Default)

h) Automatic deactivation when a MediaBridge-enhanced image is read.

i) Automatic deactivation if nothing is presented to the camera for a specified period.

j) Beep or play sound file upon reading a MediaBridge-enhanced image.

k) Blocking of sites based upon RSACi ratings. Each media owner is expected to self-rate its site using the RSACi scale for the categories of language, nudity, sex and violence. The Router blocks the end-user from a site if the RSACi rating for any category exceeds what the end-user allows. (The Router relies solely on the media owners' self-ratings and does not actually check web pages for RSACi codes.) Selecting this option also results in the display of information about RSACi (http://www.rsac.org/ratingsv01.html) regarding restricting content within the web browser.

l) Automatic connection to the Internet over an existing dial-up (modem) connection.

m) Password protection upon startup.

n) User registration information. (The user is informed that all information is optional and that specific items will be provided to third parties if provided.)

o) The end-user zip code, which the user is not required to provide, is used as a basic piece of demographic information passed along to media owners if it is voluntarily provided by the end-user.

9) **Wizard**. This wizard provides guidance in setting up a particular camera to obtain the best results with MediaBridge and the best techniques for using MediaBridge as a portal to more information. By default the wizard runs each time the Client Application is started. It also runs the first time a new camera is selected by the user.

10) **Camera verification**. When a new camera is selected as the MediaBridge Client input, the Client verifies that the camera is MediaBridge-enabled. If it is not, the user is warned that the camera is not supported and that it may not work correctly with the Client Application.

11) **Extensible architecture**. The MediaBridge Client handles reading MediaBridge-enhanced images and connecting to the desired information, usually by displaying Internet or local web pages in a

browser window. Its functionality can be extended by MediaBridge-enabled applications that register for the handling of specific data. For example, if a MediaBridge-enhanced business card were presented, the MediaBridge Client could run a MediaBridge-enabled application that downloads business card information from a web site and updates the user's contact list with the new information. Another example would be a page from a MediaBridge-enhanced children's book that causes an audio file to be played for the page.

12) **Embedding support**. If the Client Application is being used by a media owner to verify that an image has had the correct MediaBridge codes embedded in it, the Client displays the name of the media owner, the routing information and the relative strength of the MediaBridge watermark when a MediaBridge image is read. In order to protect the privacy of each media owner, this information is only provided if the user is able to provide a valid embedding user name and password for the media owner.

MediaBridge Router

The Router is essentially transparent to the end-user. When the Client Application detects a MediaBridge-enhanced image linked to information on the Internet, it communicates with the Router to obtain the Internet addressing information of the web page to be displayed.

The Router also includes the following functionality:

1) **Routing information maintenance**. Contained within the Router is information linking each unique MediaBridge code to one or more related Internet addresses. In one implementation, the system administrator (e.g., Digimarc) maintains the routing information using information supplied by its advertising customers. In another implementation, the media owners update the information themselves using a secure Internet connection with the Router.
2) **Problem handling**. If a routing request cannot be satisfied, the Router responds in a way that minimizes the impact on the end-user. For example if the MediaBridge code is unknown, then the Client Application is given the URL for the media owner's home page. In addition, each day the error occurs the Router notifies the media owner by email that the error occurred.
3) **Content rating**. If the media owner has provided RSACi rating information for the image or its site, and the end-user has specified RSACi ratings that specify that the site is to be blocked, the Router returns a web page to the user indicating that the site contains inappropriate content and does not connect to the media owner site.
4) **Validation**. Periodically (e.g., on a daily basis) the Router validates all of the active information in its database. If any errors are found, the media owners are notified by email. If the errors are not fixed with one day, Digimarc is notified. The conditions checked are:
   a) Missing URLs on active links.
   b) URLs referring to non-existing pages.
   c) Pages that exceed the acceptable download time as required by Digimarc.

5) **Tracking**. The Router may log Client Application requests in order to develop marketing information. Such a tracking log could include:

a) Date and time of the request.

b) Media owner and image.

c) Zip code of the end-user, if provided.

d) IP address that issued the request.

6) **Reporting**. Using the tracking information, the Router provides the following reports for use by Digimarc:

a) Number of URL requests for a particular date range.

b) Number of URL requests by media owner for a particular date range.

c) Number of URL requests by MediaBridge-enhanced image for a particular date range.

(The tracking and reporting are desirably structured to allow media owners to obtain traffic and marketing reports online from the Router.)

MediaBridge Embedding System

The Embedding System includes:

- a Photoshop-compatible Embedder Plug-in for embedding the MediaBridge codes,
- a Photoshop-compatible Reader Plug-in for verifying MediaBridge-enhanced digital images,
- the Client Application for verifying MediaBridge-enhanced proof and press prints, and
- an Internet-based Router Maintenance Application for obtaining MediaBridge codes and assigning URLs to MediaBridge codes.

The Plug-ins require a connection to the Internet only for authorization and to assign new MediaBridge routing codes. The Router Maintenance Application always requires an Internet connection.

Router Maintenance Application

The Router Maintenance Application's primary purpose is to assign routing information to the MediaBridge codes so that an end-user is presented with the appropriate web page when the Client Application reads an image.

The Router Maintenance Application includes the following functionality:

1) **Multiple locations**. A single media owner account can be accessed by different people in different locations. It can also be accessed by people in different organizations such as by an advertiser and its advertising agency.

2) **Restricted Access**. Each media owner has the ability to restrict who can access the Router information and can specify who can create new MediaBridge codes, use existing MediaBridge codes, or change the information for routing codes. The media owner can add, change or revoke access at any time.

3) **Secure access.** All Internet access to the Router is through secure connections.
4) **Routing Codes.** The assignment of new routing codes, changing existing routing and deleting or reusing old routing codes.
5) **Time-based routing.** Each routing code can be assigned multiple URLs, each of which can optionally have an effective date and an expiration date that determines when it is to be used in routing. Expired URLs may automatically be deleted by the router after thirty days.
6) **Multiple routing.** If multiple URLs are specified for a routing code, the Router returns to the end-user a browser-based menu that allows the end-user to chose what page to display, rather than directly navigating to a web page. In one embodiment, a single routing code may have up to four unexpired URLs. Each URL can have a short description that will be a browser link to the URL, a long description of up to 500 characters, and a URL to an icon to be displayed in the menu. The icon can be no larger than 50 pixels high by 300 pixels wide.
7) **Logging.** All changes to the routing information are logged and may be reviewed by the media owner.

Plug-in Overview

The first time embedding is done on a computer for a media owner, the Embedder requires the account number for the media owner, and a valid user name and password as defined by the media owner. The Embedder connects via the Internet to the Router, verifies that the user is authorized, and downloads information about the media owner. Further embedding for that media owner can be performed without connecting to the Router. However, each time the user connects to the Router to obtain routing information for embedding, the Router validates the user name and password against the currently valid names and passwords. If the previously used name and password are no longer valid, the user has to provide a valid name and password in order to continue embedding for the media owner.

The media owner account number is only needed for the initial authorization since any future verification is done using the name of the media owner as maintained by the Embedder. Since a graphics artist at an advertising agency can work on projects for two or more media owners, a single graphics artist may have different user names and passwords for each media owner.

The Reader Plug-in is used primarily for verification of images after embedding. It restricts access in the same way as the Embedder Plug-in with the additional restriction that it will provide information about an image only if the user can provide a valid user name and password for the media owner. If the media owner information is not available on the current computer, the Reader will connect to the Router for verification.

The plug-ins share this functionality:

1) **Multiple media owners.** A user can perform embedding or reading for multiple media owners. The user must have a valid user name and password for each media owner.
2) **Multiple users.** A single computer can be used by several people. Unless they are using the same user name and password, they do not share information.

3) **Automatic Software Update.** The user can automatically install updates to the plug-ins by making a simple menu choice. The plug-ins connect to the Internet, and download and install any available updates.

4) **Secure access.** All Internet access is through secure connections.

Embedder Plug-in

The Embedder Plug-in also includes the following functionality:

1. **Routing codes assignment.** The user selects a routing code to embed from a list of existing codes provided by the Router via an Internet connection. Each routing code is identified by a unique routing number and description. Once selected through the Router the information about a routing code is retained on the local computer until removed by the user.
2. **New routing codes.** If authorized, the user can connect to the Router through the Embedder to create a new routing code. The routing code can be created with or without the URL information, which can be added later.
3. **Routing code updates.** Whenever the Embedder connects to the Router, it downloads any updates that were made to routing codes being cached locally.
4. **Masked embedding.** The user can mask off a part of the image so that the MediaBridge codes are only embedded in the masked area. In one embodiment, different codes are applied in different mask areas. Typically, the user cannot embed different MediaBridge codes in the same part of an image.
5. **Variable intensity.** The user can globally vary the intensity (and thus visibility) of the MediaBridge watermark from light to very heavy, and can also locally vary the intensity in different areas of an image (i.e., the intensity is adapted to local image characteristics).
6. **Logging.** Each time the user embeds in an image, the Embedder records a log of the date, time, information embedded, the embedding settings (e.g., intensity), the user name, the computer name, and the name of the input image file. The log is a text file on each user's computer. It can be viewed in any text editor.

Reader Plug-in

The Reader Plug-in also includes the following functionality:

1) **Reading.** Reads a digital image, which may have been scanned, and, if the user is authorized, displays the media owner, routing information and a measure of the strength of the MediaBridge watermark.

2) **Masked reading.** The user can mask off part of the image and read the MediaBridge information only from that part.

PART III

Inventive Combinations

In addition to the inventive aspects detailed earlier, some of the inventive combinations claimed in the priority cases include the following:

A1. A method comprising:

presenting a business card of an individual to an optical sensor, the optical sensor producing output data;

decoding steganographically-encoded plural-bit data from the sensor output data; and

using said plural-bit data to establish a link to an internet address having data relating to the proprietor of said business card.

A2. The method of claim A1 which includes obtaining from said internet site calendar data detailing certain activities of the individual.

A3. The method of claim A2 in which the amount of calendar data obtained depends on an authorization level.

A4. The method of claim A3 in which the authorization level is reflected in the plural-bit data encoded in the individual's business card, wherein an individual can distribute differently-encoded cards to different recipients, to grant the recipients different access rights to said calendar data.

A5. The method of claim A1 in which the optical sensor is a business card reader that also serves to input textual information from business cards into a personal information manager.

A6. The method of claim A5 which includes storing an internet address discerned from the steganographically-encoded plural-bit data into said personal information manager.

A7. The method of claim A1 in which the optical sensor is a digital camera.

A8. The method of claim A7 in which the digital camera is mounted to a computer display device.

A9. The method of claim A7 in which the digital camera is head-mounted on a user thereof.

A10. A method comprising:

presenting a printed promotion to an optical sensor at a first site, the optical sensor producing output data;

decoding steganographically-encoded plural-bit data from the sensor output data;

using said data to establish a link to an internet site relating to a company, product, or service promoted by said printed promotion; and

transferring to from the internet site to the first site additional information relating to said company, product, or service.

A11. A method comprising:

presenting a printed identification badge to an optical sensor, the optical sensor producing output data corresponding to optical characteristics of the face of said badge;

decoding steganographically-encoded plural-bit data from the sensor output data;

checking the plural-bit data to determine whether it corresponds to a valid access card; and

unlocking a lock depending on the outcome of the foregoing checking operation.

B1. A method comprising:

presenting a digitally encoded object to an optical sensor, the optical sensor producing output data;

decoding plural-bit data from the sensor output data; and

using said plural-bit data to establish a link to an internet address having data relating to said object.

B2. The method of claim B**Error! Reference source not found.** in which the object is steganographically encoded with said plural-bit data.

B5. An apparatus comprising

a refrigerator;

an optical sensor associated with the refrigerator, the sensor being adapted to provide image data corresponding to an object held in front of the sensor; and

an image processor for processing the image data and extracting plural-bit binary data therein;

wherein the apparatus is useful for compiling a listing of groceries.

B6. In a method of operating a computer, the computer including an operating system with a registry database, the registry database associating specific data types with specific software programs particularly corresponding thereto, an improvement comprising:

providing a frame of image data;

decoding plural-bit identifier data from the image data;

consulting the registry database to identify a software program corresponding to said identifier data; and

invoking the identified software program.

B7. The method of claim B6 which includes:

steganographically decoding plural fields of data from the image data, one of said fields comprising the identifier data; and

providing another of said fields of data to the identified software program for use thereby.

B8. A system for responding to an object encoded to convey plural-bit auxiliary data, the system including:

an optical capture device that produces image data corresponding to a field of view, the field of view including visual clutter as well as the object;

a visual clue-based subsystem for identifying the object from the visual clutter in the image data; and

a processor for extracting the plural-bit auxiliary data from the object as identified by said subsystem and for applying the extracted auxiliary data to a response system.

B9. The system of claim B8 in which the visual clue-based subsystem identifies the object from the visual clutter by reference to a spectral attribute.

B10. The system of claim B8 in which the object includes a retro-reflective member, and the system includes a source of illumination of spectral character that is reflected off the retro-reflective member and detected by the optical capture device.

B11. The system of claim B8 in which the visual clue-based subsystem identifies the object from the visual clutter by reference to a temporal attribute.

B14. A method of producing an object customized to authorize a person's entry to a first location, comprising:

providing the person an access code;

generating printable data in which the access code is steganographically encoded; and

using a printer at a second location remote from the first location to print said printable data.

B15. The method of claim B14 in which the access code is provided to the person via a networked computer, and the first location is a theater.

B16. A printer responsive to commands from printer driver software, the printer driver software being characterized by being responsive to two types of input data, one of said types comprising text data, the other of said types comprising watermark data, the two types being separately applied to the printer driver software, rather than integrated together prior to application to the printer driver software.

B17. In a method of producing printed output using a computer, the printed output comprising text, the computer including software, the software presenting a print dialog box in response to user control, an improvement wherein the print dialog box has a graphical user interface permitting the user to select steganographic encoding of the printed output.

B18. A method of printing magazines, comprising:

processing blank pages to steganographically encode plural bit data thereon;

thereafter, printing text and/or imagery on the processed pages to yield steganographically-encoded printed magazine pages; and

binding at least one of said steganographically-encoded printed magazine pages into each of plural magazines.

B19. A method of travel promotion, comprising:

steganographically encoding a travel photograph to hide plural-bit data therein;

processing the travel photograph to extract the plural-bit data therefrom;

using at least part of the extracted plural-bit data to direct an internet web browser to a web site that provides travel information useful to a consumer who wishes to visit the location depicted in the photograph.

B21. A gestural method for providing input to a system, comprising:

holding an object in the hand of a user, positioning the object to be at least partially within the field of view of an optical scanning device, and manually moving said object;

with the scanning device, grabbing frames of image data plural times per second;

processing the frames of image data to identify the object as represented therein;

analyzing the representation of the object in the frames of image data to detect change over time in at least one parameter selected from the list consisting of: rotation state, scale state, differential scale state, and X-Y offset; and

controlling some aspect of the system in accordance with said detected change.

B22. The method of claim B21 in which:

the object is digitally-encoded;

the method includes decoding plural-bit digital data from the object; and

the system is responsive to at least some of said decoded digital data.

B23. The method of claim B21 in which the system responds to at least some of said decoded digital data by setting a level of sophistication of the system-user interaction accordingly.

B24. The method of claim B21 which includes analyzing the representation of the object in the frames of image data to detect change over time in rotation state, and controlling some aspect of the system in accordance with said detected change.

B25. The method of claim B21 which includes analyzing the representation of the object in the frames of image data to detect change over time in scale state, and controlling some aspect of the system in accordance with said detected change.

B26. The method of claim B21 which includes analyzing the representation of the object in the frames of image data to detect change over time in differential scale state, and controlling some aspect of the system in accordance with said detected change.

B27. The method of claim B21 which includes analyzing the representation of the object in the frames of image data to detect change over time in X-Y offset, and controlling some aspect of the system in accordance with said detected change.

B28. The method of claim B21 which includes analyzing the representation of the object in the frames of image data to detect a first change over time in one of said parameters, and thereafter to detect a second change over time in one of said parameters, and controlling some aspect of the system in accordance with said detected changes.

B29. The method of claim B21 in which the first and second changes both relate to the same parameter.

B30. In a method of operating a telephone-like appliance that establishes a voice circuit between a caller and a recipient, an improvement comprising: presenting to an optical sensor a substrate having indicia thereon, imaging a field of view that includes at least part of the substrate and producing image data corresponding thereto, steganographically decoding plural-bit digital data from the image data, and establishing the voice circuit in accordance with at least some of said plural-bit digital data.

B31. The method of claim B30 in which the indicia comprises a photographic image depicting the recipient.

B32. A method comprising:

positioning an identity object to be at least partially within the field of view of an optical scanning device, the identity object being selected from the list consisting of: a driver's license, a government identity document, a bank card, and an item of signet jewelry;

with the scanning device, grabbing a frame of image data;

processing the image data to steganographically decode plural-bit data therefrom; and

providing at least some of said steganographically decoded data to a computer system.

B33. The method of claim B32 that further includes obtaining email data from an email account corresponding to a person identified by the identity object, and providing same to a user of the computer system.

B34. An email data terminal for use in public places, the terminal including an input and an output, the output providing email data to users thereof, an improvement wherein the input includes an optical scanning device for generating scan data corresponding to an identity object, the identity object being selected from the list consisting of: a driver's license, a government identity document, and bank card.

B35. A promotional method comprising:

presenting an object within the field of view of an optical sensor device, the object being selected from the list consisting of a retail product, or packaging for a retail product;

acquiring optical data corresponding to the object;

decoding plural-bit digital data from the optical data;

submitting at least some of said decoded data to a remote computer; and

determining at the remote computer whether a prize should be awarded in response to submission of said decoded data.

B36. A method of tailoring the desktop of a first computer to conform to a user's preferences, comprising:

presenting an identity object to an optical sensor associated with the first computer;

analyzing image data produced from the optical sensor to decode plural-bit data therefrom; and

tailoring the computer desktop in accordance with said decoded data.

B37. The method of claim B36 that further includes:

using at least part of said decoded data in communicating from said first computer to a remote computer, the remote computer having profile data stored thereon relating to the user's preferred desktop arrangement;

transferring said profile data from the remote computer to the first computer; and

arranging the desktop on the first computer in accordance with said profile data.

B38. A method comprising:

purchasing a product or service from a first vendor;

receiving evidence of the purchase;

presenting the evidence to an optical scanning device to produce image data;

decoding plural-bit data from the image data;

employing said decoded plural-bit data to derive value from a second vendor unrelated to the first.

B39. The method of claim B38 in which the value is the provision of a free, or discounted, product or service from the second vendor.

B40. A method comprising:

presenting a travel document to an optical scanning device, the travel document having plural-bit data encoded thereon, the optical scanning device providing image data corresponding thereto;

discerning the plural-bit data from the image data; and

based on said plural-bit data, establishing a link to a remote computer, and employing said computer to alter travel plans.

B41. A communications method comprising:

presenting a business card to an optical sensor, the optical sensor producing image data, the business card corresponding to a person;

discerning from the image data plural-bit digital information;

using said discerned digital information to access a remote data store;

obtaining from the data store updated contact information for the person; and

establishing communication with the person using said updated contact information;

wherein the contact information at the remote data store is updated during the day as the person's activities make different contact information appropriate at different times.

B42. The method of claim B41 in which the plural-bit digital information is steganographically encoded on the business card.

B44. A method comprising:

presenting a physical object within the field of view of an optical sensor associated with a first computer, the optical sensor providing image data;

decoding plural-bit digital data from the representation of the physical object within said image data;

using a first part of said plural-bit digital data to establish a link between the first computer and a remote computer;

presenting a second part of said plural-bit digital data to the remote computer; and

providing information from the remote computer to the first computer, said information corresponding to said physical object.

B45. The method of claim B44 which includes using the first part of said plural-bit digital data to traverse a network of plural server computers to thereby identify the remote computer.

B46. The method of claim B44 in which the object is a business card relating to a person, and the information provided from the remote computer includes contact information relating to said person.

B47. A method comprising:

steganographically encoding a print advertisement with auxiliary data;

publishing said advertisement;

charging a fee for said publishing to an advertiser;

providing technology by which the steganographic encoding can be exploited to provide enhanced value to the advertiser; and

sharing a portion of said fee with a provider of said technology.

B48. A method comprising:

steganographically embedding a plural-bit digital identifier in a photograph;

storing an annotation in a database in association with said identifier;

presenting the photograph to an optical sensor, the optical sensor providing image data

decoding the identifier from the image data;

using the decoded identifier to access the annotation stored in the database; and

presenting the accessed annotation.

B49. A method of navigating the internet comprising:

linking to an internet address using a computer, and presenting information to a user of the computer from said address;

presenting an object to an optical sensor associated with the computer, the sensor producing image data corresponding to a field of view;

physically manipulating the object within said field of view;

discerning the manipulation of the object from the image data and producing output data corresponding thereto; and

changing the internet address in accordance with said output data, to thereby change the information presented to the user.

B50. A note pad comprising several sheets removably joined to each other at one edge by adhesive, characterized in that each sheet is encoded with plural-bit digital data.

B51. The note pad of claim B50 in which each sheet is steganographically encoded with plural-bit digital data.

B52. The note pad of claim B50 in which each sheet is encoded with the same plural-bit digital data as other sheets in the pad.

B53. A method comprising:

presenting an object to an optical sensor, the optical sensor producing image data, the object being steganographically encoded with plural bits of digital data;

decoding said digital data from the image data; and

in response to said digital data, storing image data from said sensor depicting the object.

B54. The method of claim B53 in which the object is a sheet of paper and the method includes

capturing several frames of image data from the optical sensor;

identifying one of said frames as having a suitable representation of the object;

masking image data corresponding to the sheet from other image data in the identified frame;

processing the image data corresponding to the sheet to change a geometrical attribute thereof;

discerning the size and color of the sheet from certain of said digital data decoded therefrom; and

storing the masked, processed image data corresponding to the sheet in association with data indicating the date and time at which the image was stored, together with the size and color of the sheet.

B55. A method comprising:

presenting an object to an optical sensor, the optical sensor producing image data, the object being steganographically encoded with plural bits of digital data;

decoding said digital data from the image data; and

in response to said digital data, displaying an image of a like object.

B56. The method of claim B55 in which the object is a sheet of paper, and the method includes displaying images of plural sheets of paper earlier stored, in a display order corresponding to the temporal order in which they were earlier stored.

B57. In a computer operating system, a software module responsive to successive frames of two-dimensional image data to extract gesture data therefrom, the gesture data including at least two data from the list consisting of: X-Y position data, rotation state, scale state, and differential scale state.

C1. A communications method comprising:

presenting a business card to an optical sensor, the optical sensor producing image data, the business card corresponding to a person;

discerning from the image data plural-bit digital information;

using said discerned digital information to access a remote data store;

obtaining from the data store updated contact information for the person; and

establishing communication with the person using said updated contact information;

wherein the contact information at the remote data store is updated during the day as the person's activities make different contact information appropriate at different times.

C2. The method of claim C1 in which the plural-bit digital information is steganographically encoded on the business card.

C3. A method comprising:

presenting a physical object within the field of view of an optical sensor associated with a first computer, the optical sensor providing image data;

decoding plural-bit digital data from the representation of the physical object within said image data;

using a first part of said plural-bit digital data to establish a link between the first computer and a remote computer;

presenting a second part of said plural-bit digital data to the remote computer; and

providing information from the remote computer to the first computer, said information corresponding to said physical object.

C4. The method of claim C3 which includes using the first part of said plural-bit digital data to traverse a network of plural server computers to thereby identify the remote computer.

C5. The method of claim C3 in which the object is a business card relating to a person, and the information provided from the remote computer includes contact information relating to said person.

D1. A method comprising:

presenting a digitally encoded object to an optical sensor, the optical sensor producing output data;

decoding plural-bit data from the sensor output data; and

using said plural-bit data to establish a link to an internet address having data relating to said object.

D2. The method of claim D1 in which the object is steganographically encoded with said plural-bit data.

E1. A promotional method comprising:

steganographically encoding a print advertisement to hide plural-bit data therein;

processing the print advertisement to extract the plural-bit data therefrom;

using at least a part of the extracted plural-bit data to direct an internet web browser to a web site that provides consumer information related to a product or service promoted by the print advertisement.

E2. A method of determining consumer response to print advertising, comprising:

steganographically encoding a first print advertisement with first data;

steganographically encoding a second print advertisement with second data;

decoding the first and second data when consumers present the first and second advertisements to an optical sensor; and

tallying the number of decoded first and second data, respectively, to determine consumer response to the advertisements.

E4. A method of travel promotion, comprising:

steganographically encoding a travel photograph to hide plural-bit data therein;

processing the travel photograph to extract the plural-bit data therefrom;

using at least part of the extracted plural-bit data to direct an internet web browser to a web site that provides travel information useful to a consumer who wishes to visit the location depicted in the photograph.

F1. In a mouse having X- and Y- position encoders, and circuitry responsive thereto for generating X- and Y- movement data and providing same to an associated computer, an improvement comprising an optical sensor disposed in said mouse, and circuitry responsive thereto for producing grey-scale optical image data and for providing same to the associated computer, wherein the mouse serves both as a positioning device and as an optical input device.

F2. A semiconductor comprising:

a substrate having formed thereon:

a two dimensional image sensor for producing sensor signals;

first circuitry responsive to said sensor signals for producing image data corresponding thereto, and for providing said image data to an image data output of said semiconductor;

second circuitry responsive to said sensor signals or to said image data for steganographically decoding plural-bit digital data therefrom, and for providing same to a steganographic decoder output of said semiconductor.

F3. In a method of operating a computer system that includes an internet web browser, an improvement comprising:

providing a peripheral device having a sensor;

positioning the peripheral device adjacent a first object to direct the web browser to a first address; and

positioning the peripheral device adjacent a second object to direct the web browser to a second address.

G1. A peripheral device for a computer system comprising:

a housing adapted to fit within a user's palm and slide over a medium;

an optical sensor having plural sensing elements and producing image signals;

a lens for imaging the medium onto the sensor;

circuitry coupled to the sensor and disposed within the housing for processing the signals from the sensor and formatting same as frames of output data; and

transfer means for relaying the output data from the peripheral device to the computer system.

G2. The device of claim G1 in which the transfer means is a cable.

G3. The device of claim G1 in which the transfer means is a wireless link.

G4. The device of claim G1 in which the circuitry decodes plural bit binary data that is steganographically encoded within image sensed by the sensor, and the transfer means relays the decoded data to the computer system.

G5. An electronic commerce method comprising:

providing a printed catalog that includes an image of an article offered for sale by a merchant, wherein the image is steganographically encoded with plural-bit binary data;

optically sensing the image to produce image data corresponding thereto;

decoding the steganographically encoded data from the image data; and

electronically ordering the article from the merchant by use of said decoded data, wherein said ordering makes use of earlier-stored customer profile information.

G6. The method of claim G5 in which the customer profile information includes clothing size data.

G7. The method of claim G6, further comprising:

processing the decoded data for transmission to a remote merchant computer, said processing including supplementing the decoded data with supplemental data corresponding to the customer;

transmitting the processed data to the remote merchant computer;

receiving first order data from the remote merchant computer, responsive to the transmitted processed data;

presenting the first order data to the customer;

receiving from the user further input selecting among options included in the first order data; and

transmitting said further input to the remote merchant computer.

G8. The method of claim G7 in which the supplemental data includes the customer profile information.

G9. The method of claim G7 in which the supplemental data includes data identifying the customer.

G10. An access control device comprising:

a badge;

a photograph on the badge;

the photograph having plural-bit auxiliary data hidden therein, said auxiliary data corresponding to an authorized bearer of the badge;

the badge further including further bearer-identification information, said further information being machine-detectable.

G11. The device of claim G10 in which the further information is encoded by an RF proximity circuit formed with the badge.

G12. The device of claim G10 in which the further information is encoded in a bar code on the badge.

G13. The device of claim G10 in which the further information is encoded in a magnetic stripe on the badge.

G14. A method of accessing a secured premise comprising:

presenting a badge to a sensor station;

generating optical data corresponding to a photograph on the badge;

processing the optical data to extract plural-bit auxiliary data steganographically encoded therein;

machine-sensing the ID of the badge from data not encoded in the photograph; and

checking correspondence between the machine-sensed ID and the auxiliary data extracted from the photograph to determine whether access to the secure premise is authorized.

I1. An image-based navigation system, comprising:
an optical input device;
a client application responsive to digital data encoded in an image; and
a router responsive to at least a part of said digital data.

I2. A computer storage medium having instructions thereon for causing a camera-equipped computer system to engage in a training exercise with a user to familiarize the user with operation of a camera-based internet navigation system.

I3. An internet navigation device comprising a substrate having an image printed thereon, the image having first and second data encoded therewith, the first data comprising an owner code, the second data comprising a router code, said device being useful in linking a camera-equipped computer system to an internet address.

I4. The device of claim I3 in which the owner and router codes are steganographically encoded in the image.

I6. An image-based network navigation method permitting a user to link to a remote computer, comprising:
detecting encoded data from a printed image;
linking to the remote computer through a network in accordance with said encoded data; and
providing an identity of the image to the remote computer.

I7. In an internet navigation system comprising a client application in communication with a remote router, a method comprising:
providing first data from the client application to the router;
providing plural data from the router to the client application;
at the client application, presenting a menu corresponding to said plural data; and
accepting user input corresponding to one of said plural data.

I8. The method of claim I7 that includes deriving the first data from image data provided from an optical input device.

I9. The method of claim I8 that includes linking the client application to a web page corresponding to the accepted user input.

I10. The method of claim I9 that includes presenting to a user a branded display locally stored at the client application while waiting for the linked web page to display.

I11. A router that accepts a routing code and responds with a URL corresponding thereto, characterized in that at least one routing code corresponds to plural URLs, each of which has temporal information detailing when the URL is to be used.

J2. A database method comprising:

generating a database record including plural data fields;

generating a file corresponding to said database record and including data from at least certain of said fields;

electronically distributing a copy of the file to each of plural recipients;

one of said recipients adding data to a copy of the file, or changing data in a copy of the file, and sending the file to the database;

updating the database record in accordance with said changed file;

generating a new file corresponding to the updated database record and including data from at least certain of said fields; and

electronically distributing a copy of the new file to each of said plural recipients.

J3. A system for linking from physical or digital objects to corresponding digital resources, comprising:

registration means for receiving data relating to an object, including its identity and owner, and associating same in a database with data relating to a corresponding response;

originating device means for sensing data from an input object, processing same, and forwarding same to a routing means;

routing means for processing the processed data from the originating device means, logging information from same, and forwarding at least certain of said processed data to a product handler means; and

product handler means for providing a response to the originating device means in accordance with the information provided thereto by the routing means.

J4. The system of claim J3 in which the routing means includes means for checking information in the database.

J5. The system of claim J3 in which the registration means includes means for generating an encapsulating file and means for distributing said file to predetermined parties.

J13. A networked computer system, responsive to watermark data sent from a remote client application to initiate delivery of audio or video data.

J14. The networked computer system of claim J13, responsive to watermark data sent from a software program on a remote computer, to initiate delivery of audio or video data to said remote computer.

J16. A networked computer system, responsive to watermark data sent from a software program on a remote computer, to initiate delivery of updated software to said remote computer.

K1. In a scanner including a CPU, a memory, a linear sensor array, and first and second spaced-apart 2D sensor arrays serving as motion encoders, the CPU serving to process raw scan data collected by the linear sensor array from an imaged object into final scan data in accordance with scanner motion data provided from said 2D sensors, an improvement comprising software instructions in the memory causing the scanner to discern a machine-readable identifier from scan data acquired from the object.

K2. The scanner of claim K1, further comprising a wireless interface, and a display, said software instructions causing the scanner to relay the identifier by the wireless interface to a remote server, and for processing information returned through the wireless interface for presentation on said display.

K3. The scanner of claim K1 in which the software instructions cause the CPU to process data from the 2D sensor arrays for a purpose in addition to sensing scanner motion.

K4. The scanner of claim K3 in which said purpose includes beginning a watermark detection process before data from the linear sensor array is finally processed.

K5. The scanner of claim K4 in which said purpose includes beginning to sense a watermark calibration signal.

K6. The scanner of claim K3 in which said purpose includes identifying portions of the data collected by the linear sensor array that are relatively more likely to include detectable identifier data.

K7. The scanner of claim K3 in which said purpose is to quantify an object surface characteristic, wherein a filter can be applied to the scan data in accordance therewith.

K8. The scanner of claim K3 in which said purpose is to assess relative distance to the object from different portions of the scanner.

K9. The scanner of claim K3 in which said purpose is to quantify an affine distortion in the scan data, so that compensation may be applied therefore.

K10. The scanner of claim K1 in which the identifier is steganographically encoded as a digital watermark.

K11. The scanner of claim K1 in which the identifier is encoded as a barcode.

K12. A scanner comprising a linear sensor array, a CPU, an interface for coupling to the internet, and a user interface including a display screen and user controls, the scanner being adapted to transmit machine-readable data sensed from scanned objects to the internet, and for presenting to a user HTML information received back from the internet.

L1. In an image watermarking technique that includes changing an optically-sensible pattern on an object, an improvement wherein the object has a non-planar surface, and the watermark applied to said surface is pre-warped to precompensate for said non-planarity.

L2. The method of claim L1 in which the watermark is geometrically pre-warped.

L3. The method of claim L1 in which the object has a cylindrical surface.

L4. The method of claim L3 in which the object is a container for consumer goods.

L5. The method of claim L4 in which the object is a soft drink can.

L6. The method of claim L1 in which the watermark is pre-warped in a transform domain.

L7. The method of claim L6 in which the watermark is pre-warped in the wavelet domain.

L8. The method of claim L6 in which the watermark is pre-warped in the DCT domain.

L9. The method of claim L1 in which the watermark is pre-warped to account for a curvature-induced apparent geometrical distortion.

L10. The method of claim L1 in which said surface is pre-warped to account for a distance-induced apparent geometrical distortion.

L11. The method of claim L10 in which the watermark is pre-warped to account for a curvature-induced apparent geometrical distortion.

L12. In watermark decoding technique that includes analyzing a frame of image data to decode a watermark encoded therein, an improvement comprising applying an unwarping function to the image data prior to decoding the watermark.

L13. The method of claim L12 which includes successively applying different unwarping functions to the image data to attempt to decode valid watermark data therefrom.

L14. The method of claim L12 which includes selecting one or more unwarping functions to apply based on information provided by a user.

L15. The method of claim L14 in which said information identifies a general class of objects to which the object belongs, without specifically identifying a specific object shape.

Conclusion

Having described and illustrated the principles of our technology with reference to illustrative embodiments, it should be recognized that the invention is not so limited.

For example, while certain of the embodiments were illustrated with reference to internet-based systems, the same techniques are similarly applicable to any other computer-based system. These include non-internet based services such as America Online and Compuserve, dial-up bulletin board systems, etc. Likewise, for internet-based embodiments, the use of web browsers and web pages is not essential; other digital navigation devices and other on-line data repositories can be similarly accessed.

Similarly, while the details of illustrative systems were particularly given, the underlying principles can be employed in numerous other forms.

For example, one other form is to steganographically encode physical objects with Digital Object Identifiers (DOIs). The Center for National Research Initiatives and the Digital Object Identifier Foundation (www.doi.org) have performed extensive work in establishing an infrastructure by which digital objects can be distributed, tracked, and managed. Some of this same infrastructure and technology can be adapted, in accordance with the teachings provided above, to associate new functionality with physical objects.

Another form is not to reference a remote data repository by data embedded on an object, but instead to encode the ultimate data directly on the object. A photograph, for example, can be literally encoded with a telephone number. On presenting the photograph to an optical sensor on the telephone, the telephone can analyze the optical information to extract the telephone number, and dial the number, without the need for any external data. Similarly, a printed office document (e.g., spreadsheet) can be encoded with the path and file name of the corresponding electronic file, obviating the need for indirect

linking (e.g., to a remote database to correlate a UID to a computer address). A person's business card can directly encode that person's email or web address. Most of the above-described embodiments are suitable for such direct encoding of the related data.

In the business card example given above, the detailed techniques can be supplementary to existing optical character recognition techniques. That is, the image data from an optical sensor can be applied both to a Bedoop decoder and to an OCR system. Text characters discerned by the OCR system can be entered directly into a contacts manager personal database. The techniques employed in the Bedoop system to locate the encoded object and handle visual distortion (e.g., the visual artifacts due to scale, rotation, etc.) can advantageously be used in OCR detection as well, permitting extraction of the OCR information without careful placement of the card.

While certain of the foregoing embodiments made reference to ink-jet printing, similar advantages can often be obtained with other printing technologies, e.g., laser/xerographic printing, offset printing, etc.

In the foregoing embodiments, Bedoop decoding generally proceeded from image data obtained from a physical object. However, in some contexts, it is advantageous to Bedoop-decode image data provided electronically, e.g., over the internet.

Likewise, while the foregoing embodiments generally relied on Bedoop image sensors that stared out for an object at an expected point, in alternative embodiments, sensors that seek rather than stare can be employed (as was illustrated above in connection with the elevator example).

Similarly, while the illustrated embodiments generally employed sensors that repeatedly grabbed frames of image data, this need not be the case. Single frame systems, such as flatbed scanners, and video systems arranged to grab single frames -- with or without TWAIN interfaces -- can alternatively be used.

As indicated above, while steganographic encoding of the digital data is used in the preferred embodiments, visible forms of digital encoding – such as bar codes – can naturally be employed where aesthetic considerations permit.

In certain of the embodiments, digital data conveyed by means other than optical can be used. Electromagnetic detection (e.g., of the sort used in proximity-based card-access systems) can be arranged to decode digital data, permitting "at-a-distance" reading of data from physical objects, just as in the foregoing embodiments.

Since the Bedoop image sensors typically acquire plural frames of data, the extraction of the digital data can be based on more than a single image frame. More confidence in the results may be accumulating decoded data over several frames. Moreover, movement of the object within the sensor's field of view may permit the system to acquire information from other perspectives, etc., enhancing system operation.

While the preferred embodiments employ 2-D image sensors (e.g., CCDs), other optical sensing technology can alternatively be employed. Supermarket laser scanners, for example, can read bar-code

data. Raster-scanning of such systems can permit acquisition of 2-D data (either in bit-mapped form, or grey-scale).

Some embodiments can advantageously employ texture-based Bedoop encoding of objects. Bedoop texturing can be effected by various means, including pressure rollers, chemical or laser etching, etc.

It should be noted that the responses triggered by a watermark can be changed over time. This extends the useful life of an encoded object. For example, an encoded link in a magazine ad for a 1999 Ford Explorer that points to a Ford URL related to the 1999 Ford Explorer can be updated to point to the URL for the 2000 model year version when marketing of the new model year vehicles commences.

In other embodiments, of course, a literal URL can be encoded, and can be used to direct a browser or other information appliance to that address. Still further, a literal URL can be encoded, but not necessarily used. Instead, the encoded URL can be mapped to an actual URL (i.e., a URL to which the browser is directed or to which a response to the MediaBridge object is otherwise keyed) through a database. In one such embodiment, a URL is encoded in an object together with a future date. On "reading" the object, the local (client) computer checks the associated date. If the date has not passed, the literal URL is used as the actual URL. If the date has passed, the client computer refers to the code to a remote database (e.g., at the router) to obtain an actual URL (which may be the same – if no update has been required, or may be new). The actual URL is then used in providing a response to the MediaBridge object.

The implementation of the watermark encoding and decoding systems is straightforward to artisans in the field, and thus not unduly belabored here. Conventionally, such technology is implemented by suitable software, stored in long term memory (e.g., disk, ROM, etc.), and transferred to temporary memory (e.g., RAM) for execution on an associated CPU. In other implementations, the functionality can be achieved by dedicated hardware, or by a combination of hardware and software. Reprogrammable logic, including FPGAs, can advantageously be employed in certain implementations.

While the foregoing embodiments have generally employed planar objects to convey the digital encoding, this need not be the case. Objects of other shapes can likewise be employed. Some shapes present relatively straightforward image processing tasks. As noted above, data imaged from a soft drink can or other cylindrical surface can be remapped using known geometrical transforms so as to essentially "unwrap" the printing from the can. Other geometries can present more complex re-mappings, but are likewise generally within the capabilities of the artisan. (Such remapping is facilitated by encoding in the data certain reference markings, such as subliminal graticules, etc. The unknown 3D shape of the object being imaged can usually be inferred from the apparent warping of the reference markings in the 2D image data generated by the scanner. Once the warping is characterized, it is generally straightforward to un-warp so as to prepare the image data for decoding.)

It was once popular to predict that paper documents would be replaced with electronic media. In hindsight, electronic media may be recognized as a poor surrogate for paper. Electronic media conveys information flawlessly, but is lacking in experiential attributes. We can hold paper, stack it,

own it, deface it, give it, guard it, etc. It provides an opportunity for physical dominion entirely lacking with electronic media.

From the foregoing discussion it can be seen that, rather than replacing paper with electronic media, perhaps the future lies in giving paper digital attributes – hybridizing the physical experience of paper with the technical advantages of digital media. Such an arrangement makes available a great wealth of new functionality, now accessible through familiar paper items, rather than through a "computer input peripheral."

To provide a comprehensive disclosure without unduly lengthening this specification, applicants incorporate by reference the patents, applications, and publications identified above.

In view of the many embodiments to which the above-detailed principles may be applied, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of our invention. Rather, we claim as our invention all such embodiments as fall within the scope and spirit of the following claims, and equivalents thereto.

WE CLAIM

1. A method of data processing on a computer system, comprising:

using an application program to compose an electronic version of a text-based document;

printing the document onto paper, the printing including steganographically encoding the printed paper with plural-bit auxiliary data;

storing the plural-bit auxiliary data in association with data identifying a location at which the electronic version of the document is stored.

2. A method of data processing on a computer system, comprising:

presenting a text-based printed document to an optical capture device;

processing image data produced by said device to decode plural-bit data steganographically encoded therein;

based on said decoded plural-bit data, launching a software application corresponding to said printed document; and

using said software application to open an electronic version of said document.

3. In a method of operating a computer, the computer including an operating system with a registry database, the registry database associating specific data types with specific software programs particularly corresponding thereto, an improvement comprising:

providing a frame of image data;

decoding plural-bit identifier data from the image data;

consulting the registry database to identify a software program corresponding to said identifier data; and

invoking the identified software program.

4. The method of claim 3 which includes:

steganographically decoding plural fields of data from the image data, one of said fields comprising the identifier data; and

providing another of said fields of data to the identified software program for use thereby.

5. A greeting card comprising a substrate with visually-perceptible indicia printed thereon, wherein the card is steganographically encoded with plural-bit binary data that can be decoded by an image processing device and used to direct a computer to a web site where an image, video, and/or audio presentation corresponding to said card is provided.

6. A method of providing a customized greeting, comprising:

acquiring a greeting card having plural-bit data steganographically encoded therein;

customizing a web site presentation corresponding to said card;

providing the card to a recipient;

decoding the steganographically encoded plural-bit data from the card; and

in response to said steganographically decoded plural-bit data, presenting to the recipient the web site presentation.

7. A method of printing a magazine, comprising:

processing an electronic representation of an advertisement with a digital watermark to steganographically encode plural bit data therein;

printing a page of advertising in accordance with said electronic representation to yield a steganographically encoded advertisement page; and

binding said page into a magazine;

wherein said plural bit data serves to identify an entry in a database, said database entry having stored therein an internet address of a web page that is associated with said advertisement.

8. A promotional method comprising:

steganographically encoding a print advertisement to hide plural-bit data therein;

processing the print advertisement to extract the plural-bit data therefrom; and

using at least a part of the extracted plural-bit data to direct an internet web browser to a web site that provides consumer information related to a product or service promoted by the print advertisement.

9. A method of determining consumer response to print advertising, comprising:

encoding a first print advertisement with first data;

encoding a second print advertisement with second data different than the first;

the first and second data providing identifiers by which consumer devices can link to web pages associated with said advertisements;

monitoring linking traffic due to each of said identifiers to thereby determine consumer response to the advertisements.

10. The method of claim 9 in which the encoding takes the form of visible bar codes.

11. The method of claim 9 in which the encoding takes the form of steganographic digital watermarks.

12. The method of claim 9 in which the first and second advertisements are identical, except for the data encoded therein.

13. The method of claim 12 in which the first and second advertisements are published in different magazines.

14. The method of claim 9 in which the first and second advertisements are different, apart from the data encoded therein.

15. The method of claim 14 in which the first and second advertisements are published in the same magazine.

16. A promotional method comprising:

presenting an object within the field of view of an optical sensor device, the object being selected from the list consisting of a retail product, packaging for a retail product, or printed advertising;

acquiring optical data corresponding to the object;

decoding plural-bit digital data from the optical data;

submitting at least some of said decoded data to a remote computer; and

determining at the remote computer whether a prize should be awarded in response to submission of said decoded data.

17. A method of interacting with a magazine using a computer, the computer including an internet web browser, the method including:

providing a peripheral device having a sensor;

positioning the peripheral device adjacent a first advertisement in the magazine to direct the web browser to a first internet address; and

positioning the peripheral device adjacent a second advertisement in the magazine to direct the web browser to a second internet address.

18. The method of claim 17 in which the positioning comprises scanning barcode indicia published in said advertisements.

19. The method of claim 17 in which the peripheral device is a camera device having a sensor with rows and columns of sensor elements.

20. A computer peripheral and method of its use, the peripheral being used in conjunction with a computer system having an internet browser associated therewith, the peripheral comprising:

a housing adapted to fit within a user's palm and slide over a medium;

an optical sensor having at least one sensing element and producing optical data;

a lens for imaging the medium onto the sensor;

the method comprising:

sliding the peripheral over a portion of a printed advertisement;

processing the optical data to decode plural bit information encoded on the advertisement; and

using said plural bit information to direct the internet browser to an internet web page associated with said advertisement.

21. The arrangement of claim 20 in which the plural bit information does not comprise a web address, but rather comprises an advertisement identifier, and in which the method further includes:

transmitting said advertisement identifier to a remote computer;

receiving from said remote computer a web address associated with said identifier; and

directing the internet browser on said computer system in accordance with said web address.

22. The arrangement of claim 20 which includes sliding the peripheral over a portion of the printed advertisement having a barcode printed thereon.

23. An electronic commerce method comprising:

providing a printed catalog that includes an image of an article offered for sale by a merchant, wherein the image is encoded with plural-bit binary data;

optically sensing the image to produce optical data corresponding thereto;

decoding the encoded data from the optical data; and

electronically ordering the article from the merchant by use of said decoded data, wherein said ordering makes use of earlier-stored customer profile information.

24. The method of claim 23 in which the customer profile information includes clothing size data.

25. In a wireless telephony handset including a microphone, a modulator, and an RF amplifier, the device serving to receive audio and transmit an RF signal conveying audio modulation, an improvement comprising an optical sensor producing optical data, a lens for imaging an object onto the sensor, and a decoder for decoding plural bit identifier data conveyed by a barcode or a digital watermark on the object.

26. An image-based network navigation method permitting a user to link to a remote computer, comprising:

detecting encoded data from a printed object;

linking to the remote computer through a network in accordance with said encoded data; and

providing the user's zip code to the remote computer.

27. A method comprising:

sensing an object identifier from a first object;

sending said first object identifier from a first device to a second device;

in response, at said second device, identifying address information corresponding to said first object identifier and sending same to the first device;

initiating a link from the first device in accordance with said address information;

at said second device, identifying additional objects related to said first object; identifying additional address information corresponding to said additional objects; and sending said additional address information to the first device;

storing said additional address information in a memory at the first device;

wherein, if an object included among said identified additional objects is sensed by the first device, the corresponding address information can be retrieved from said memory in the first device without the intervening delays of communicating with the second device.

28. An apparatus including a detector of machine readable data and a software program used in conjunction with said machine readable data, operable to transmit a packet of data to a remote system, said packet of data comprising (a) an identifier of said software program, and (b) at least a portion of detected machine readable data.

29. The apparatus of claim 28, wherein said packet of data also includes address information identifying the apparatus.

30. The apparatus of claim 28 comprising a detector of digital watermark data.

31. The apparatus of claim 28 comprising a detector of barcode data.

32. An apparatus including a detector of machine readable data and a software program used in conjunction with said machine readable data, operable to transmit a packet of data to a remote system, said packet of data comprising (a) a context or environment identifier, and (b) at least a portion of detected machine readable data.

33. The apparatus of claim 32, wherein said packet of data also includes address information identifying the apparatus.

34. The apparatus of claim 32 comprising a detector of digital watermark data.

35. The apparatus of claim 32 comprising a detector of barcode data.

36. A networked computer system, responsive to watermark data sent from a software program on a remote computer, to initiate delivery of advertisement data to said remote computer.

37. A system as described and detailed above.

5

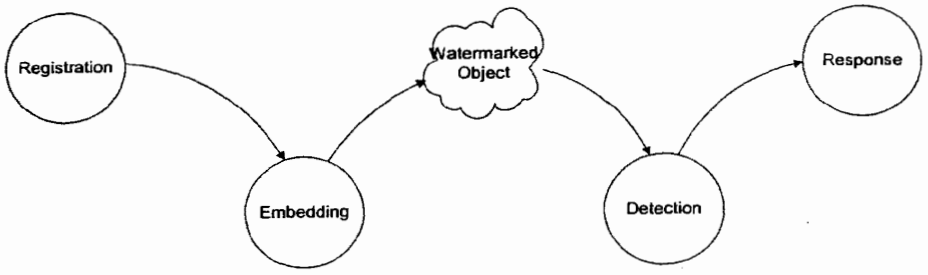

Registration
Embedding
Watermarked Object
Detection
Response

FIG. 1

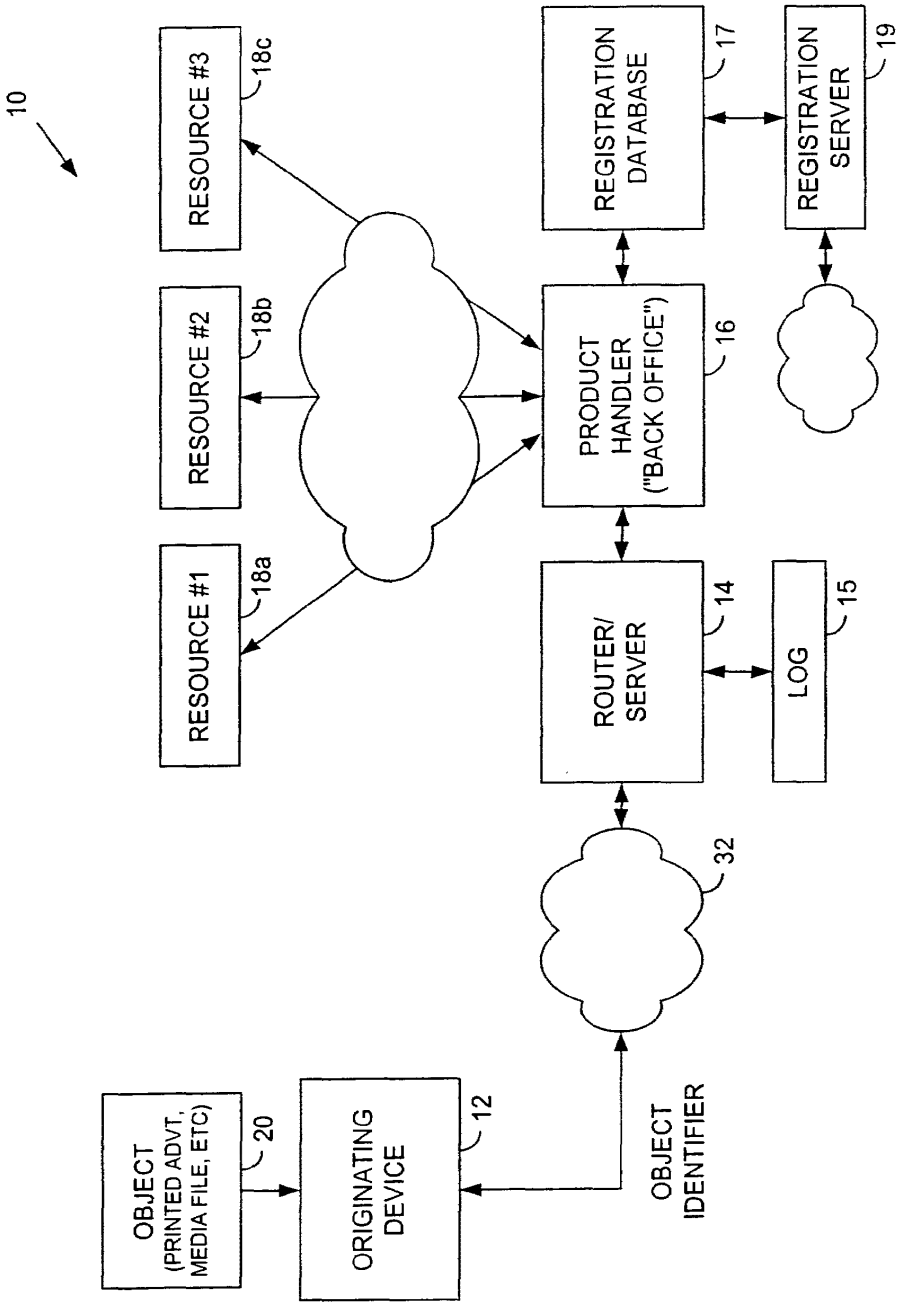

10
RESOURCE #3
18c
RESOURCE #2
18b
RESOURCE #1
18a
REGISTRATION DATABASE
17
REGISTRATION SERVER
19
PRODUCT HANDLER ("BACK OFFICE")
16
ROUTER/ SERVER
14
LOG
15
32
OBJECT (PRINTED ADVT, MEDIA FILE, ETC)
20
ORIGINATING DEVICE
12
OBJECT IDENTIFIER

FIG. 2

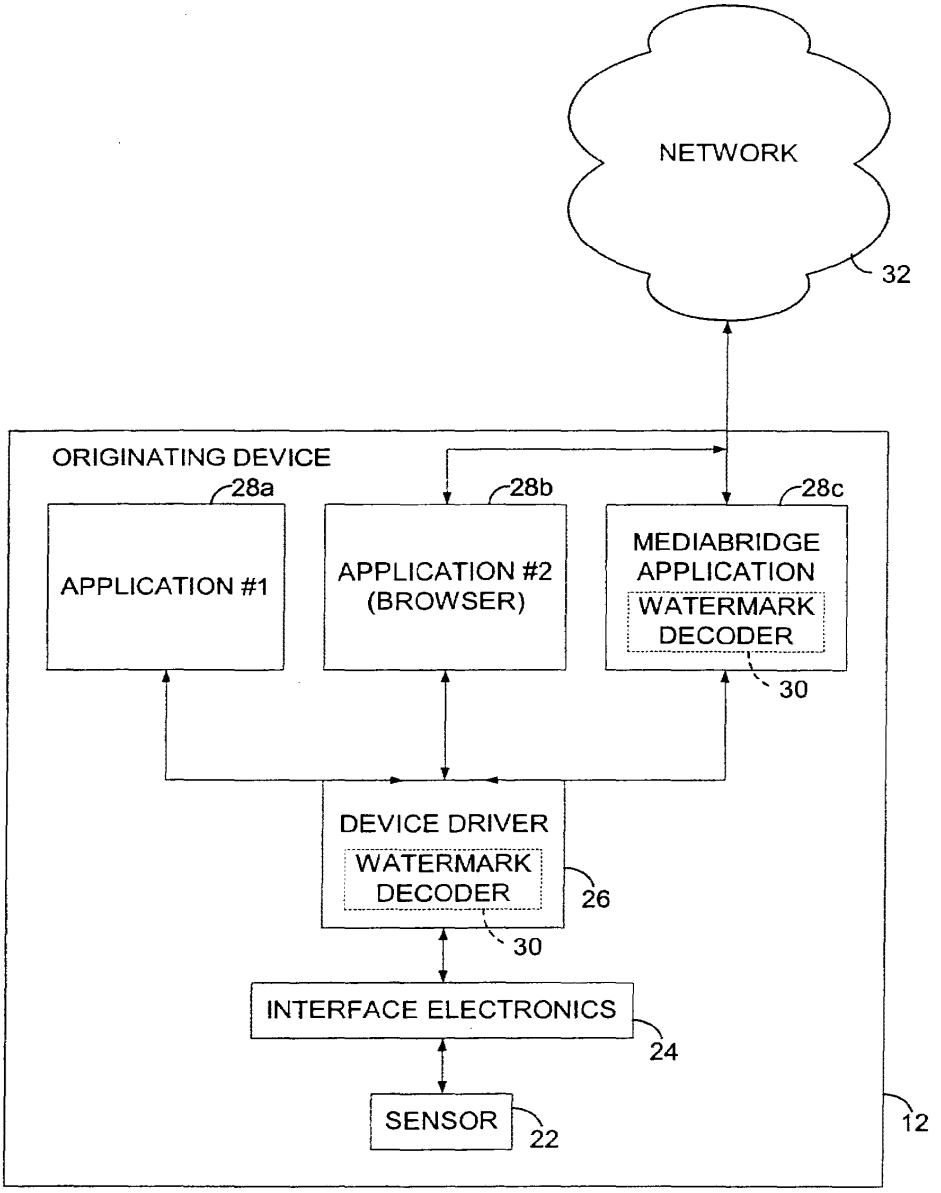

NETWORK
32
ORIGINATING DEVICE
28a
28b
28c
APPLICATION #1
APPLICATION #2
(BROWSER)
MEDIABRIDGE
APPLICATION
WATERMARK
DECODER
30
DEVICE DRIVER
WATERMARK
DECODER
26
30
INTERFACE ELECTRONICS
24
SENSOR
22
12

FIG. 3

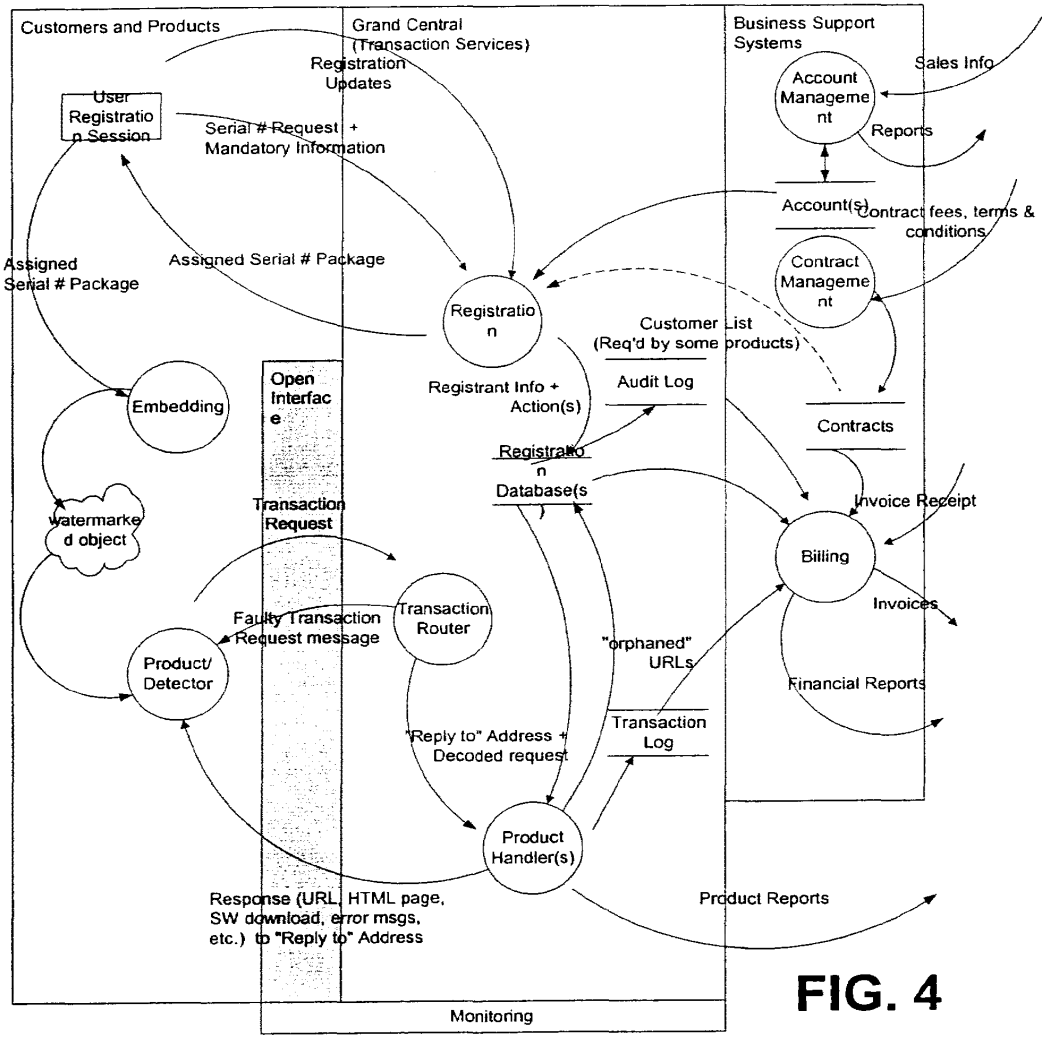


FIG. 4

SUBSTITUTE SHEET (RULE 26)

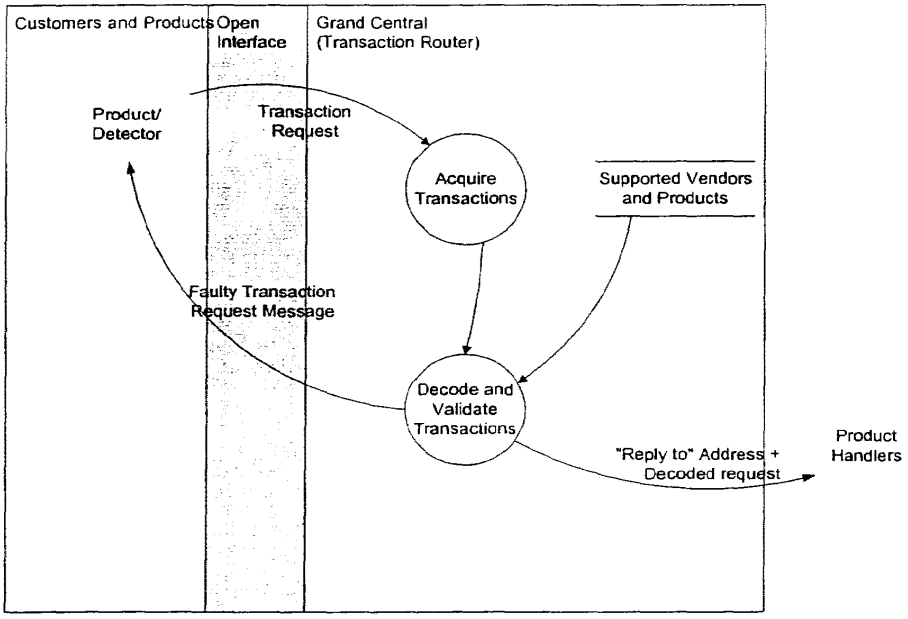


FIG. 5

Ex.1002 / Page 980 of 1311
APPLE INC.

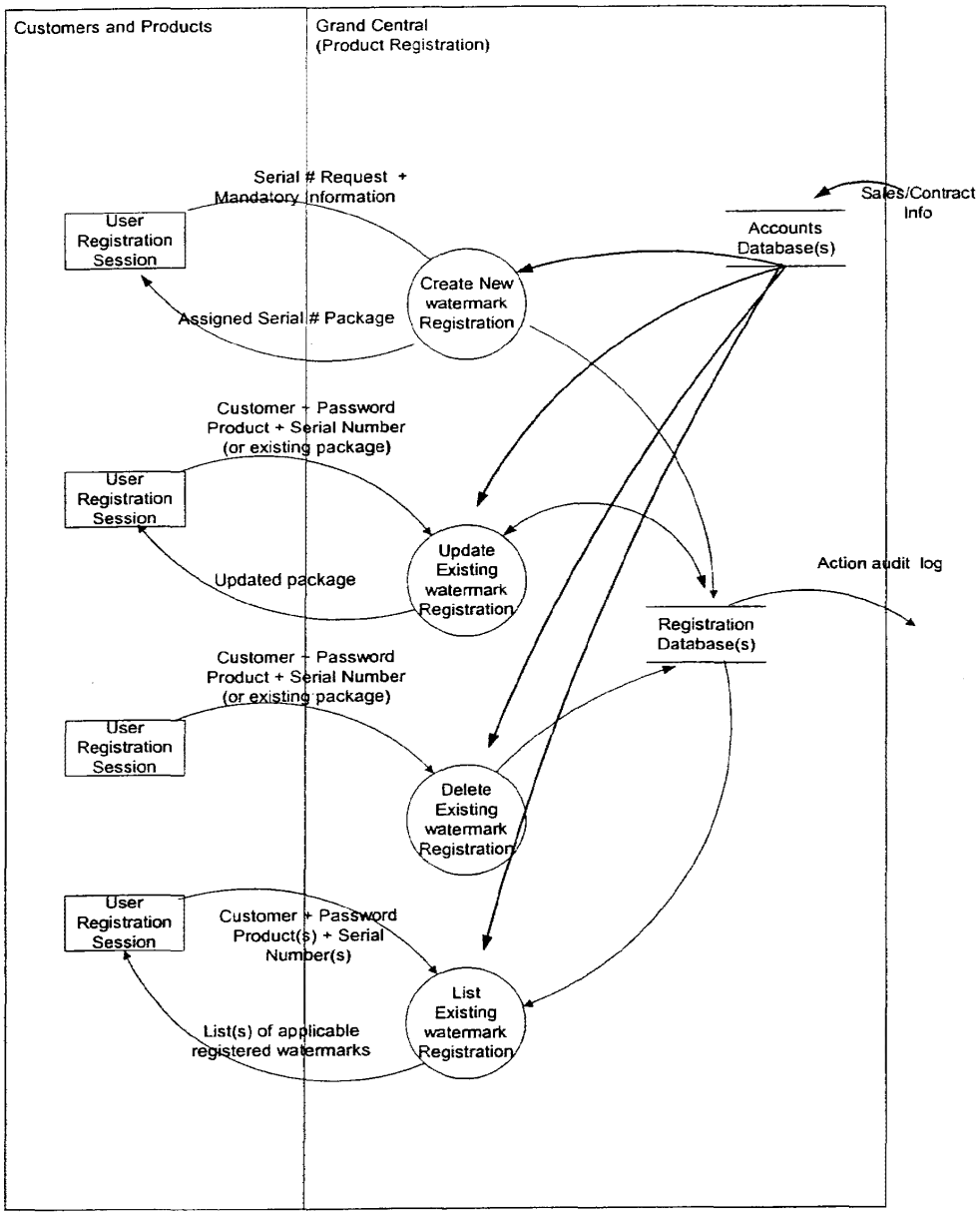

Customers and Products
Grand Central
(Product Registration)
Serial # Request +
Mandatory Information
User
Registration
Session
Assigned Serial # Package
Create New
watermark
Registration
Sales/Contract
Info
Accounts
Database(s)
Customer + Password
Product + Serial Number
(or existing package)
User
Registration
Session
Updated package
Update
Existing
watermark
Registration
Action audit log
Registration
Database(s)
Customer + Password
Product + Serial Number
(or existing package)
User
Registration
Session
Delete
Existing
watermark
Registration
User
Registration
Session
Customer + Password
Product(s) + Serial
Number(s)
List(s) of applicable
registered watermarks
List
Existing
watermark
Registration

FIG. 6

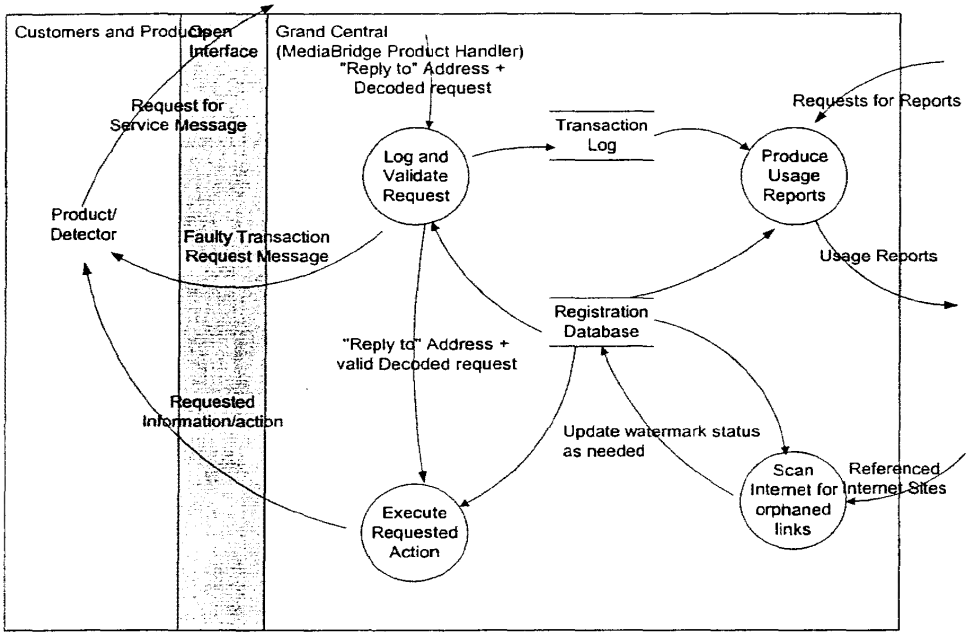

Customers and Produ
Open Interface
Grand Central
(MediaBridge Product Handler)
"Reply to" Address +
Decoded request
Request for Service Message
Transaction Log
Requests for Reports
Log and Validate Request
Produce Usage Reports
Product/ Detector
Faulty Transaction Request Message
Usage Reports
Registration Database
"Reply to" Address + valid Decoded request
Requested Information/action
Update watermark status as needed
Scan Internet for orphaned links
Referenced Internet Sites
Execute Requested Action

FIG. 7

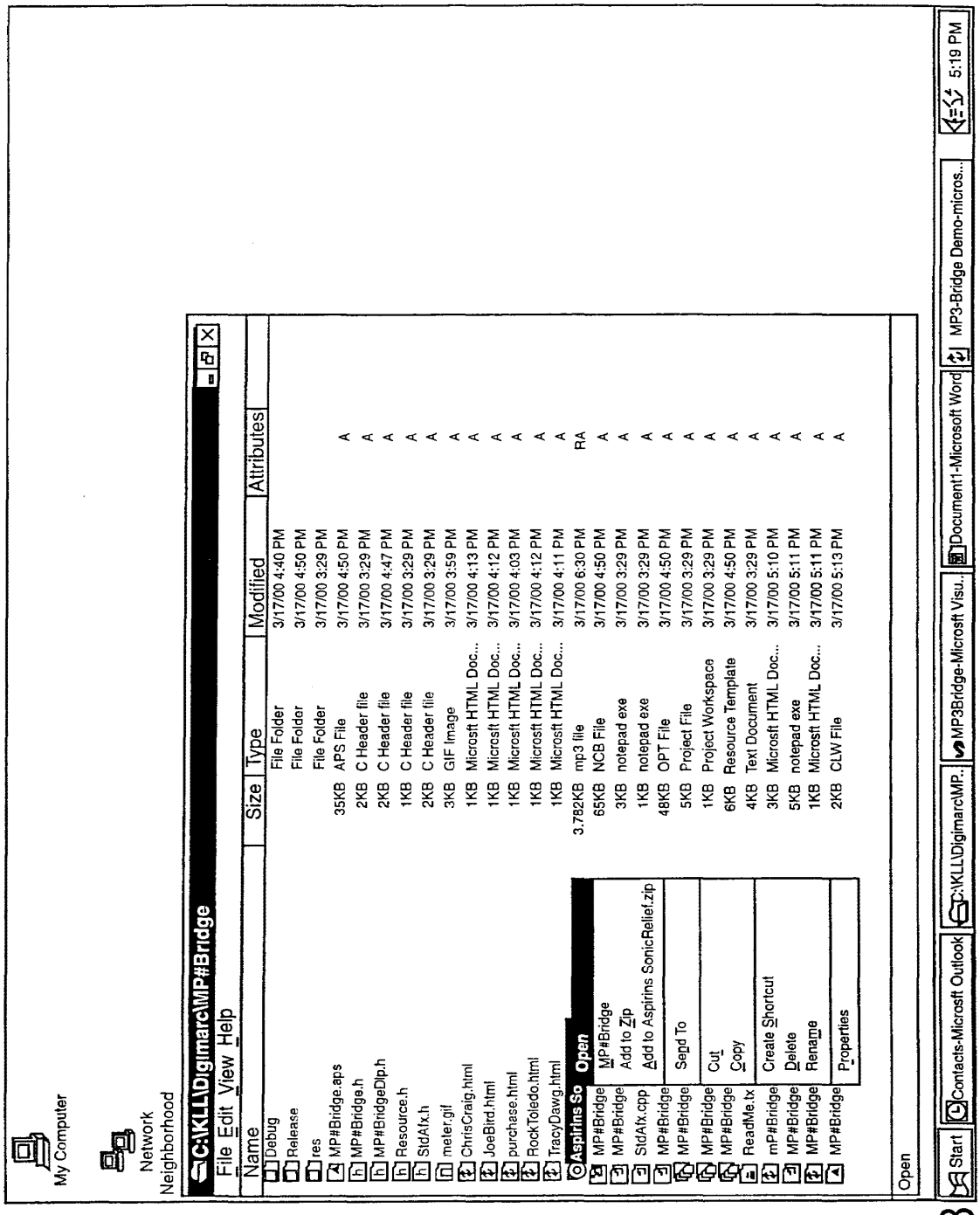
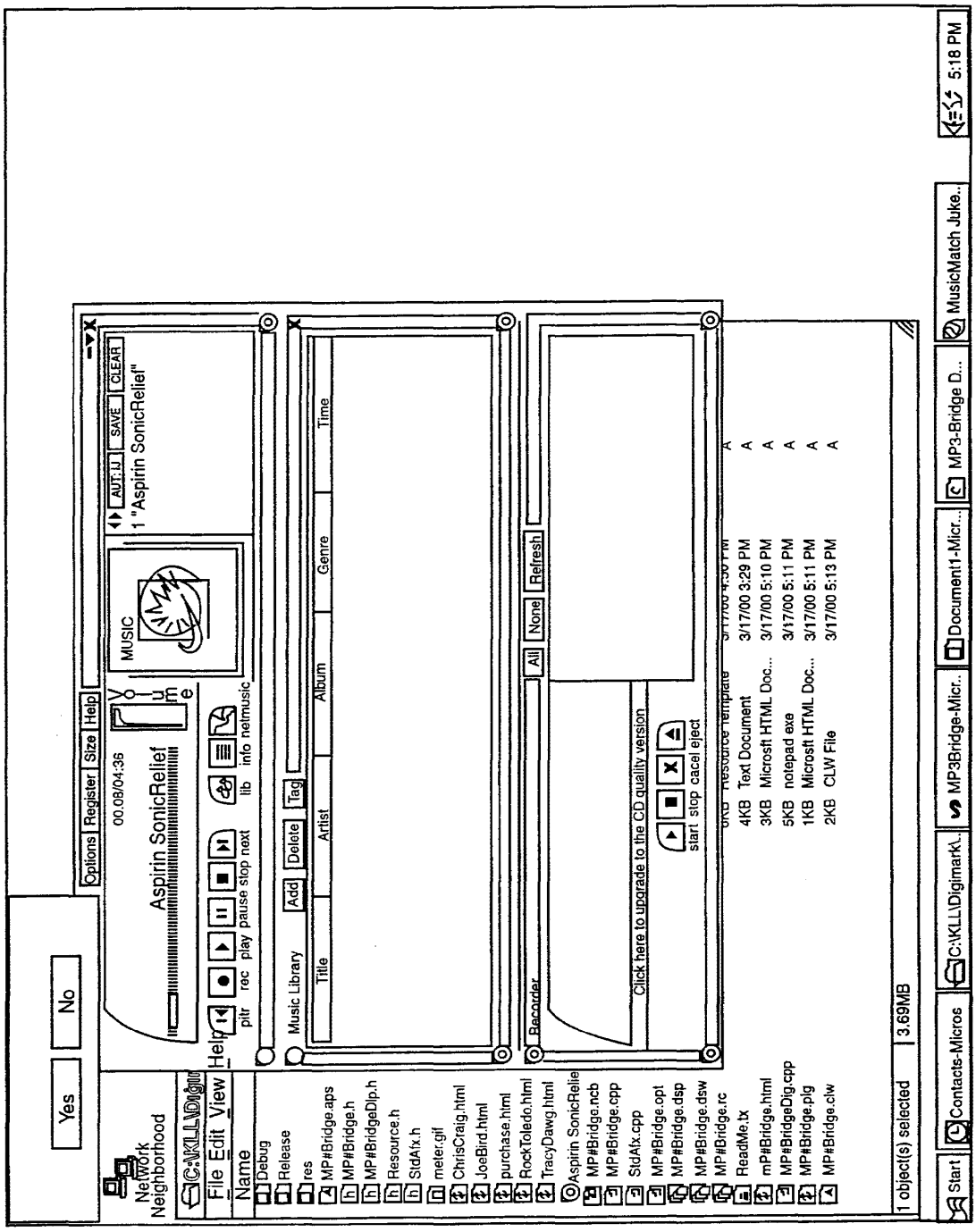

My Computer
Network Neighborhood
C:\KLLD\gimarc\MP#Bridge
File Edit View Help
Name
Size
Type
Modified
Attributes
Debug
Release
res
MP#Bridge.aps
MP#Bridge.h
MP#BridgeDlg.h
Resource.h
StdAfx.h
meter.gif
ChrisCraig.html
JoeBird.html
purchase.html
RockToledo.html
TracyDawg.html
Aspirins So
MP#Bridge
MP#Bridge
StdAfx.cpp
MP#Bridge
MP#Bridge
MP#Bridge
MP#Bridge
mP#Bridge
MP#Bridge
MP#Bridge
MP#Bridge
Open
Add to Zip
Add to Aspirins SonicRelief.zip
Send To
Cut
Copy
Create Shortcut
Delete
Rename
Properties
Open
Start
Contacts-Microsft Outlook
C:\KLLD\gimarc\MP...
MP3Bridge-Microsft Visu...
Document1-Microsoft Word
MP3-Bridge Demo-micros...
5:19 PM

FIG. 8



IG. 9

SUBSTITUTE SHEET (RULE 26)

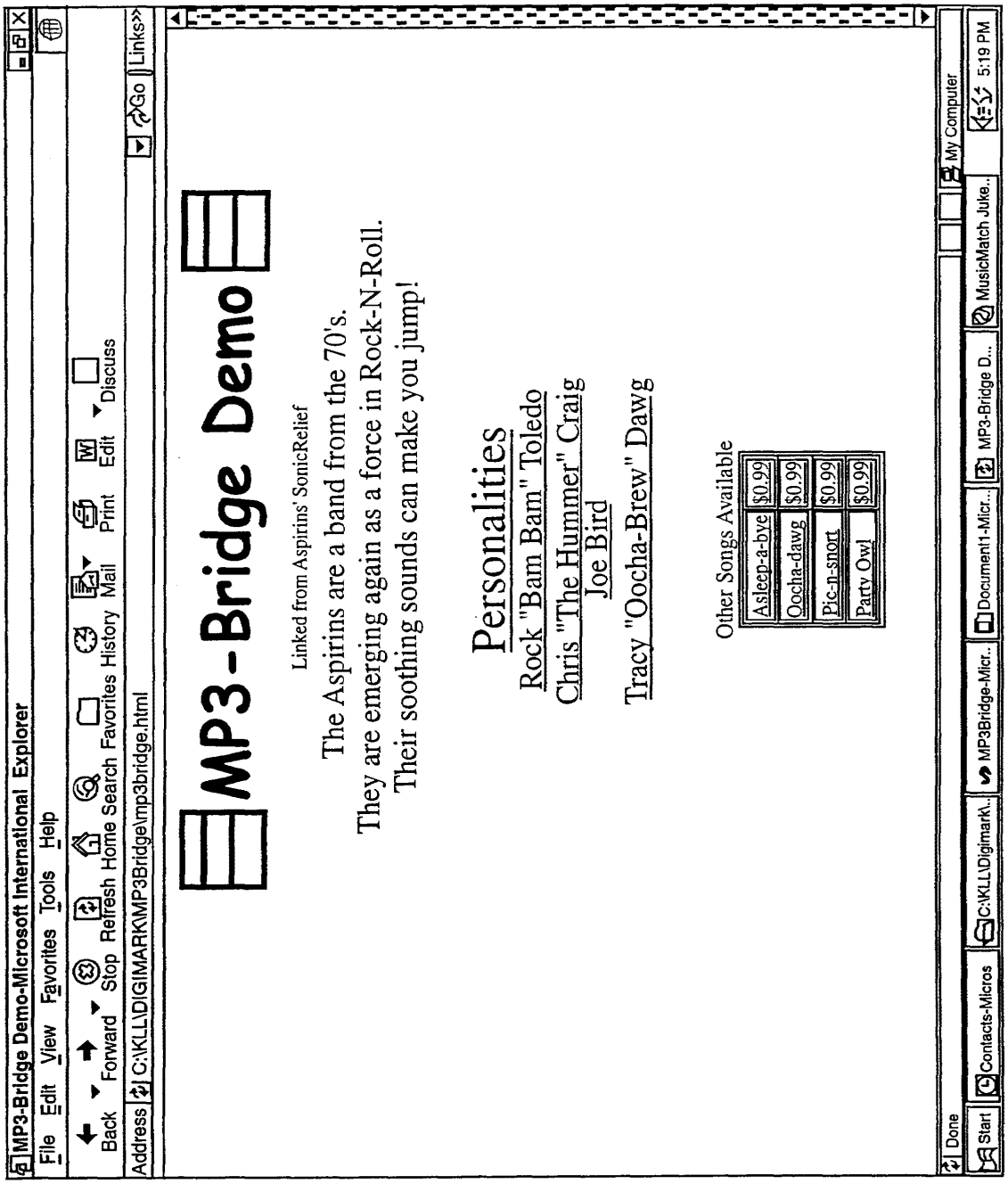

MP3-Bridge Demo-Microsoft International Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address C:\KLL\DIGIMARK\MP3Bridge\mp3bridge.html
Go Links
MP3-Bridge Demo
Linked from Aspirins' SonicRelief
The Aspirins are a band from the 70's.
They are emerging again as a force in Rock-N-Roll.
Their soothing sounds can make you jump!
Personalities
Rock "Bam Bam" Toledo
Chris "The Hummer" Craig
Joe Bird
Tracy "Oocha-Brew" Dawg
Other Songs Available
Asleep-a-bye $0.99
Oocha-dawg $0.99
Pic-n-snort $0.99
Party Owl $0.99
Done
My Computer
Start
Contacts-Micros
C:\KLL\Digimark\..
MP3Bridge-Micr..
Document1-Micr..
MP3-Bridge D...
MusicMatch Juke..
5:19 PM

FIG. 10

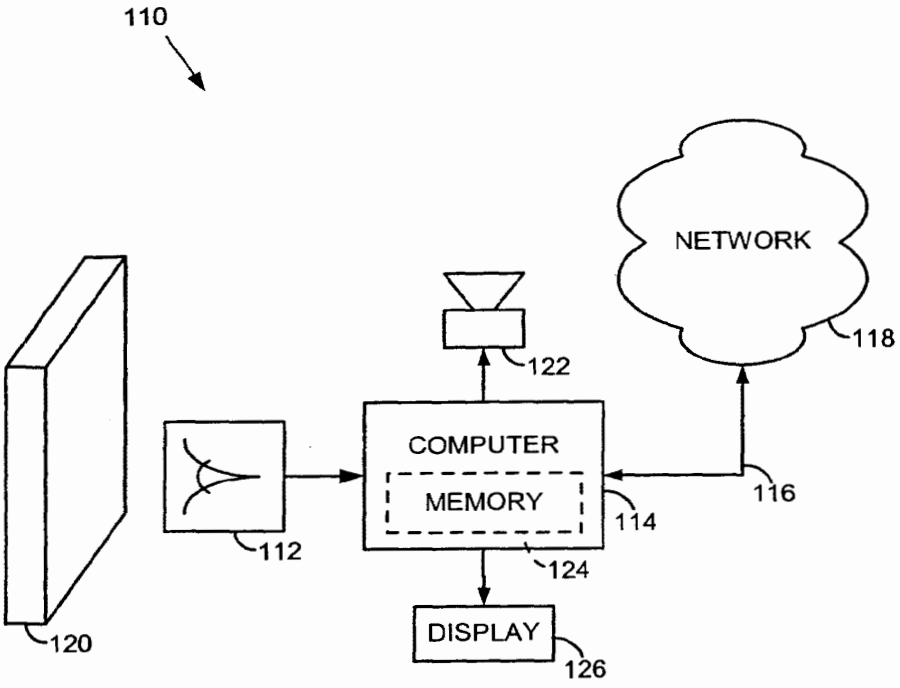
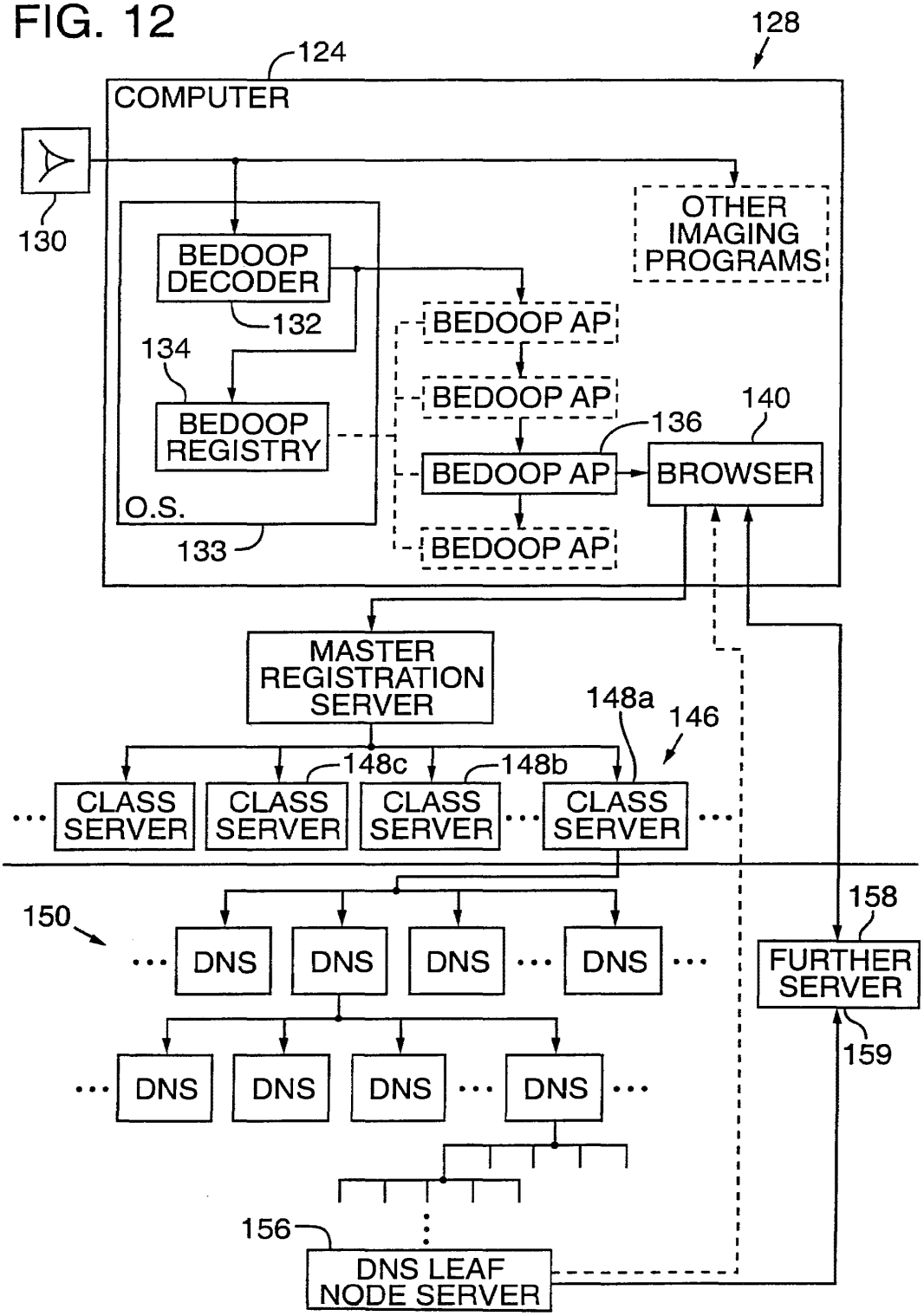

110
NETWORK
118
122
COMPUTER
MEMORY
114
116
112
124
DISPLAY
126
120

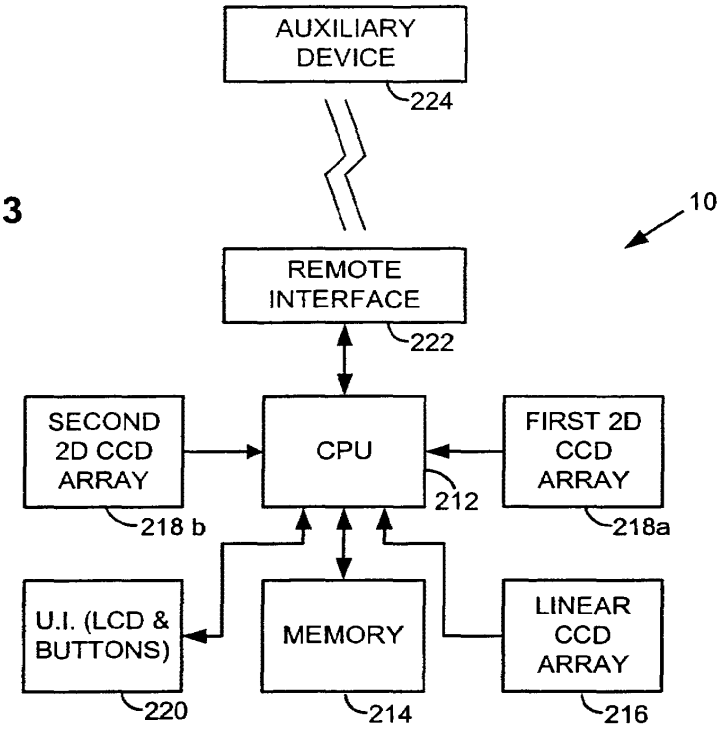
FIG. 11

FIG. 12



SUBSTITUTE SHEET (RULE 26)

FIG. 13



(Prior Art)

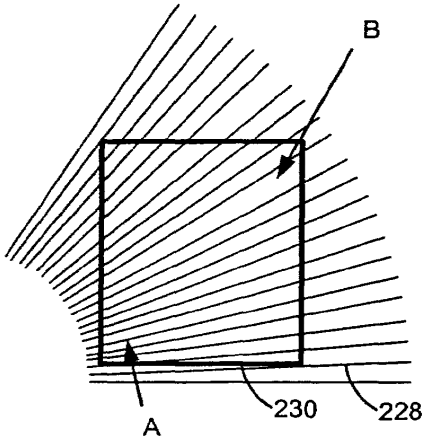


FIG. 14



Grid Orientation Under CCD 218a

Grid Orientation Under CCD 218b

FIG. 15

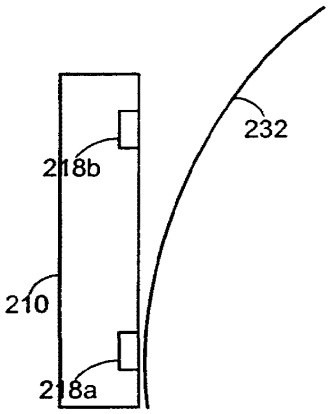


FIG. 16

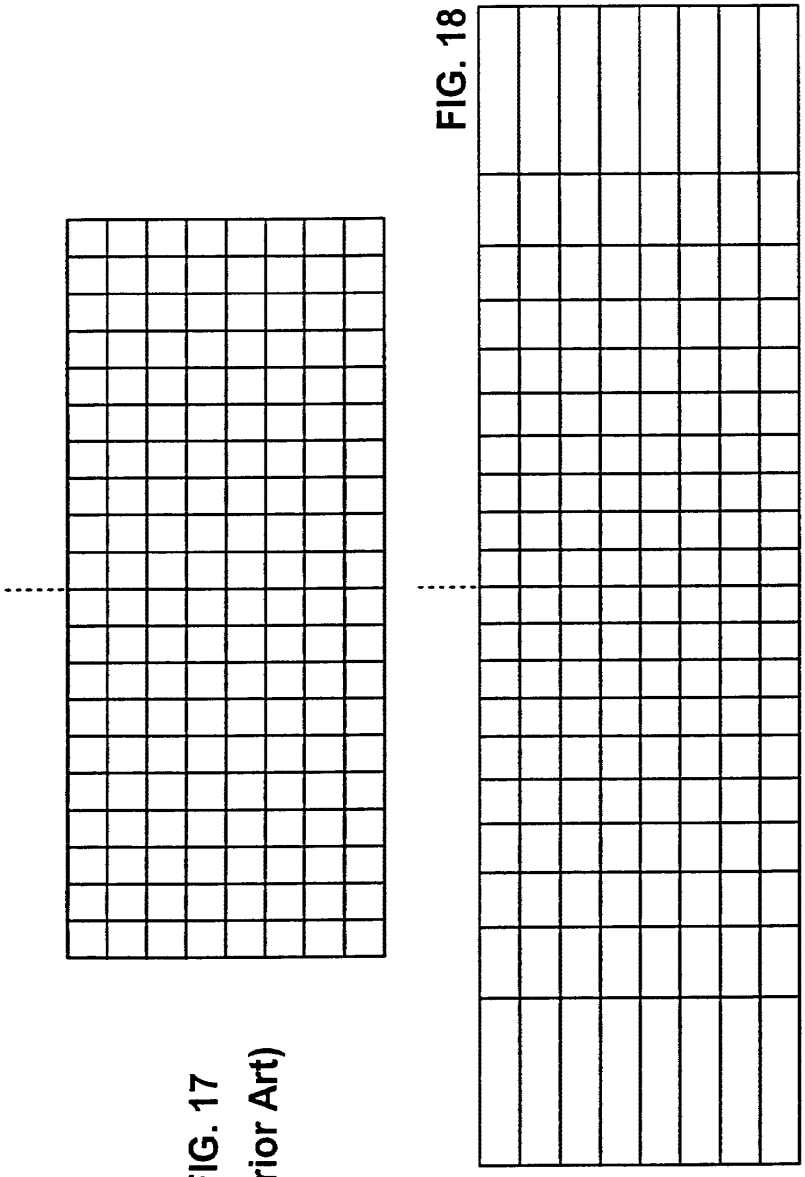


FIG. 18

FIG. 17
(Prior Art)

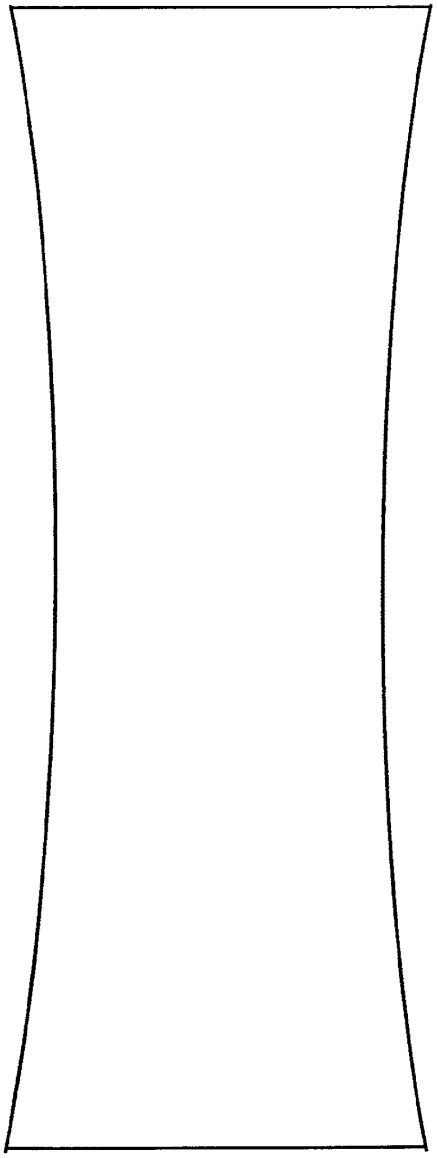


FIG. 19

Ex.1002 / Page 991 of 1311
APPLE INC.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/13333

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G09C 5/00; G06F 17/00 ; G06K 7/00, 9/00, 9/36, 19/06; H04L 9/00

US CL :Please See Extra Sheet.

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. : Please See Extra Sheet.

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.
Y	US 5,761,686 A (BLOOMBERG) 02 JUNE 1998, COL.1-24	1-36
Y, P	US 6,052,486 A (KNOWLTON ET AL.) 18 APRIL 2000, COL.2-62	1-36
A, P	US 5,930,767 A (REBER ET AL.) 27 JULY 1999, COL.1-11	1-36
A	US 5,841,886 A (RHOADS) 24 NOVEMBER 1998, COL.1-7	1-36
A, P	US 5,926,550 A (DAVIS) 20 JULY 1999, COL.2-5	1-36
A	US 5,862,260 A (RHOADS) 19 JANUARY 1999, COL.1-94	1-36

[X] 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	Date of mailing of the international search report
23 AUGUST 2000	18 SEP 2000
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 GLEN BURGE James R. Matthews Telephone No. (703) 305-4792

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/13333

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,708,717 A (ALASIA) 13 JANUARY 1998, COL.2-12	1-36
A	US 5,168,147 A (BLOOMBERG) 01 DECEMBER 1992, COL.2-19	1-36
A	US 5,278,400 A (APPEL) 11 JANUARY 1994, COL.2-5	1-36

Form PCT/ISA/210 (continuation of second sheet) (July 1998)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/13333

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. [X] Claims Nos.: 37
because they relate to subject matter not required to be searched by this Authority, namely:

It does not mean anything.

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:

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.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/13333

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

235/454, 456, 456, 494; 283/17, 57, 58, 72, 73, 85, 93; 358/429, 455; 380/30, 51, 54, 55, 243;382/115, 232; 705/26, 77; 707/529; 713/176, 193

B. FIELDS SEARCHED
Minimum documentation searched
Classification System: U.S.

235/454, 456, 456, 494; 283/17, 57, 58, 72, 73, 85, 93; 358/429, 455; 380/30, 51, 54, 55, 243;382/115, 232; 705/26, 77; 707/529; 713/176, 193

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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

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.	

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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		

EFS Web 2.1.17

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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 CORORATION		
	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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 Prorocol, 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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

	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	15272013
	Filing Date	2016-09-21
	First Named Inventor	MALONE, Michael F.
	Art Unit	2161
	Examiner Name	
	Attorney Docket Number	MPOR-33317

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)	2017-01-04
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.

Electronic Acknowledgement Receipt

EFS ID:	27971478
Application Number:	15272013
International Application Number:	
Confirmation Number:	8747
Title of Invention:	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, 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:	MPOR-33317
Receipt Date:	04-JAN-2017
Filing Date:	21-SEP-2016
Time Stamp:	17:46:21
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	Foreign Reference	EP0905966-Yoshida.pdf	2753790 eaf33d57075c4d16604e10ed0ffc65ac08559752	no	51

Warnings:

Information:					
2	Foreign Reference	WO0152178-CONWELL.pdf	2344200 e471b8df43b4fab0fb08070e92d3500d0886144e	no	48
Warnings:					
Information:					
3	Foreign Reference	WO9901859-Hayhurst.pdf	1441564 6f5690c07c87d865331baee5df26ed73e3f7227a	no	35
Warnings:					
Information:					
4	Foreign Reference	WO0167707-Bozeman.pdf	3648385 f896c8a99f500e0915482cb472efb61426248c3c	no	82
Warnings:					
Information:					
5	Foreign Reference	EP1204277A2-Tektronix.pdf	204921 707d7f27a747c5192a23be69fb87ad3bfa2c266c	no	4
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	MPO33317IDS2.pdf	612377 1a55e5a1212d417f48c5202e2edf222864a678a8	no	4
Warnings:					
Information:					
7	Foreign Reference	WO9743736A1-Digimarc.pdf	10234345 05741d3d1a842efcd6e0facb8a3927be6ff7f6e4	no	208
Warnings:					
Information:					
8	Foreign Reference	WO9626494-TheRegents.pdf	1659096 5c0110f9d3962f93ddb26773fa75eb61623f1676	no	54
Warnings:					
Information:					

9	Foreign Reference	WO9936876-Digimarc.pdf	672925 fa4c516b93d1676666c9d209e1664b57574fad96	no	22
Warnings:					
Information:					
10	Foreign Reference	WO0115021A2-DigitalConvergence.pdf	2892555 115503b27d78d5ed66bc11e70ec1832cb1e5cb3b	no	63
Warnings:					
Information:					
11	Foreign Reference	WO0161508A1-Digimarc.pdf	4310530 604fc993175179c1057cf2dd8565995e47f73386	no	68
Warnings:					
Information:					
12	Foreign Reference	WO0173586A2-DigitalConvergence.pdf	3255890 bf81cdae1de8ebbae5233009e909f53630f5d03f	no	66
Warnings:					
Information:					
13	Foreign Reference	WO0175629A1-Neomedia.pdf	1415423 cdb4617f89767647013fd19568e5dd2d9e605888	no	41
Warnings:					
Information:					
14	Foreign Reference	WO0197128A1-Markany.pdf	1640217 8a71eece8895a78310ed43b37fc452970e84c390	no	42
Warnings:					
Information:					
15	Foreign Reference	WO0211446A2-Koninklijke.pdf	1546038 4f25618de822c88b75493043cdf5ec9dee1345ae	no	33
Warnings:					
Information:					

16	Foreign Reference	WO9827510A1-TheRegents.pdf	2130470 5e373278f26f47ef19bd733fff83d02e187fd98d	no	51
Warnings:					
Information:					
17	Foreign Reference	WO0036605A1-KentRidge.pdf	1193724 7de0138cf0176a62162fc7b55ada8ea13877b539	no	27
Warnings:					
Information:					
18	Foreign Reference	WO0070585A1-Digimarc.pdf	6887558 a6bde39654a0ecf736d7706f85528c580efdac66	no	137
Warnings:					
Information:					
19	Foreign Reference	WO9603286A1-InternationalData.pdf	1552418 8b8189f80b2f6218c568275380df5ac3387646a5	no	34
Warnings:					
Information:					
20	Non Patent Literature	90013265-REQUESTreexam.pdf	10185940 d8e28f320b70255e6109c4f7a32f28bd853116ea	no	1085
Warnings:					
Information:					
21	Non Patent Literature	90013255-REQUESTreexam.pdf	9627672 15d81a27140c4a6fe6fa195dc69b67c45ecf6122	no	906
Warnings:					
Information:					
22	Non Patent Literature	90013255-RESPONSEreexam.pdf	1744129 d02e0b67a7a3e69dd918a34676c3bcf80d5e8f85	no	177
Warnings:					
Information:					

23	Non Patent Literature	90013265-RESPONSEreexam.pdf	2064944 7e6858d88a17913ceeefb30e3e55e8c3ea03abb2	no	187
Warnings:					
Information:					
24	Non Patent Literature	KRAWCZYK-HMACKeyed-Hashing.pdf	400685 477b1b9e4938fb43f6cd815b5294eff5aa0d4cc3	no	10
Warnings:					
Information:					
25	Non Patent Literature	FRIEDMAN-TheTrustworthyDigitalCamera.pdf	415682 66017d3cf20da967e9ac8fec0e9cbe4867d6000b	no	6
Warnings:					
Information:					
26	Non Patent Literature	FRANKS-AN-EXTENSION.pdf	67089 e793fa7e8c0284b4204dc664e221db325ca49fbe	no	18
Warnings:					
Information:					
27	Non Patent Literature	FRANKS-HTTP-AUTHENTICATION.pdf	67910 e4a08d7daf6718bdeb38da5e3eaec515773 6c746	no	34
Warnings:					
Information:					
28	Non Patent Literature	SupplementalFirstAmendedComplaint.pdf	447500 4c604b72408c7ec3c69dac8b7de20d0356bc74e3	no	11
Warnings:					
Information:					
29	Non Patent Literature	DigitalStillCameraImage.pdf	22047143 64617199e59c2f7931d863ff12be1e25fc31a998	no	172
Warnings:					
Information:					

30	Non Patent Literature	TIFFSpecificationRevision.pdf	4142264 b035e2c09575571375f06cb0ccd700047d4d74a7	no	121
Warnings:					
Information:					
31	Non Patent Literature	FundamentalsofGlobal-Tsui.pdf	13250703 6ba8592ff590e6d0ea25d2a1f617d3ae23df7b19	no	256
Warnings:					
Information:					
32	Non Patent Literature	PPPEncryptionControl.pdf	337027 ae6bfe22feafaa77659ca8ef01646b50ea410145	no	11
Warnings:					
Information:					
33	Non Patent Literature	AlfredMenezes-1-397.pdf	12665577 d77591c63647d8108f44ca3d528e78da9a89bbb5	no	397
Warnings:					
Information:					
34	Non Patent Literature	AlfredMenezes-398-794.pdf	14353854 fb5799dfbc1d07120aada23e3c97db140234b4bc	no	397
Warnings:					
Information:					
35	Non Patent Literature	Myportinfringementcontentions.pdf	1466955 d79e7fbe53db58f9fd91cc1a46817c858181b252	no	25
Warnings:					
Information:					
36	Non Patent Literature	STANSELL-CivilGPSfromFuturePerspective.pdf	631554 ef66654d1e8ed05058ef8cfa377744527fe89556	no	6
Warnings:					
Information:					

37	Non Patent Literature	DALE-AND-ROG.pdf	93569 01d58c16e1b4211d6a07eb5ac70f8944356ec90e	no	2
Warnings:					
Information:					
38	Non Patent Literature	KOSOVIC.pdf	2444867 d13c3dea28ef420d424ad81061f11af94c9ea32b	no	32
Warnings:					
Information:					
39	Information Disclosure Statement (IDS) Form (SB08)	MPO33317IDS1.pdf	1043850 0e8592d238c0bd8a2823ae70b4a0ee18ea94a77c	no	34
Warnings:					
Information:					
		Total Files Size (in bytes):	147895340		

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.

<u>New Applications Under 35 U.S.C. 111</u>
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.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
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.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
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.

(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)

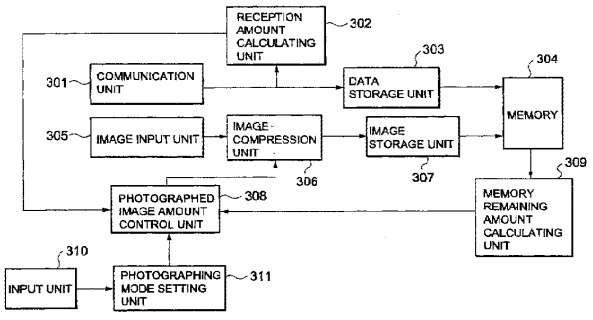
(72) Inventors:
- **Yoshida, Shigeo, Canon Kabushiki Kaisha**
  Ohta-ku, Tokyo (JP)
- **Sonobe, Hiraku, Canon Kabushiki Kaisha**
  Ohta-ku, Tokyo (JP)
- **Ono, Satoshi, Canon Kabushiki Kaisha**
  Ohta-ku, Tokyo (JP)
- **Ohara, Keiji, Canon Kabushiki Kaisha**
  Ohta-ku, Tokyo (JP)
- **Matsumoto, Shinichi, 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 1038 of 1311
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 1039 of 1311
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

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 1042 of 1311
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 1043 of 1311
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 1044 of 1311
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 1045 of 1311
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 1046 of 1311
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 1047 of 1311
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 1048 of 1311
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 1049 of 1311
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 1050 of 1311
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 1051 of 1311
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 1052 of 1311
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 1053 of 1311
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 1054 of 1311
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 1055 of 1311
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 1056 of 1311
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 1057 of 1311
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 1058 of 1311
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 1059 of 1311
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 1060 of 1311
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 1061 of 1311
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 1062 of 1311
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 1063 of 1311
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 1064 of 1311
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 1065 of 1311
APPLE INC.

FIG.1

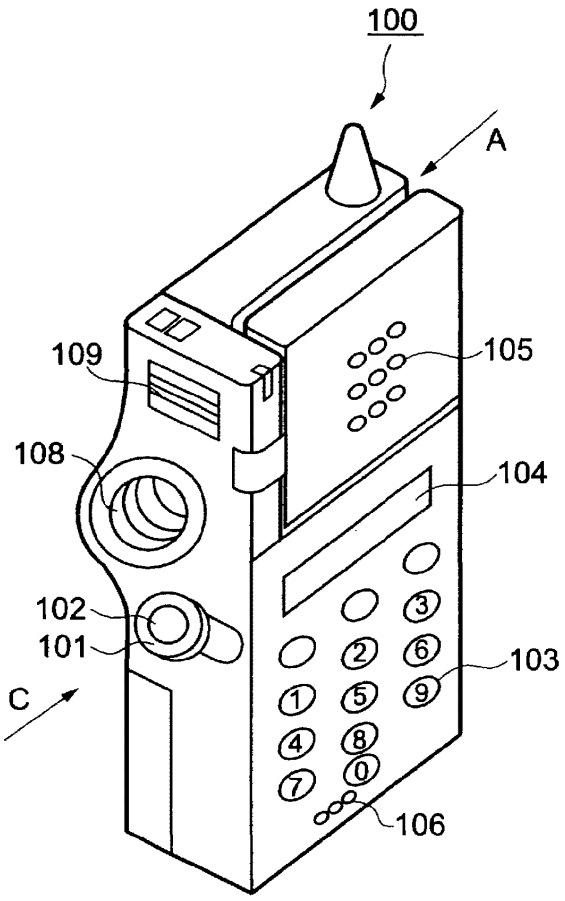


FIG.2

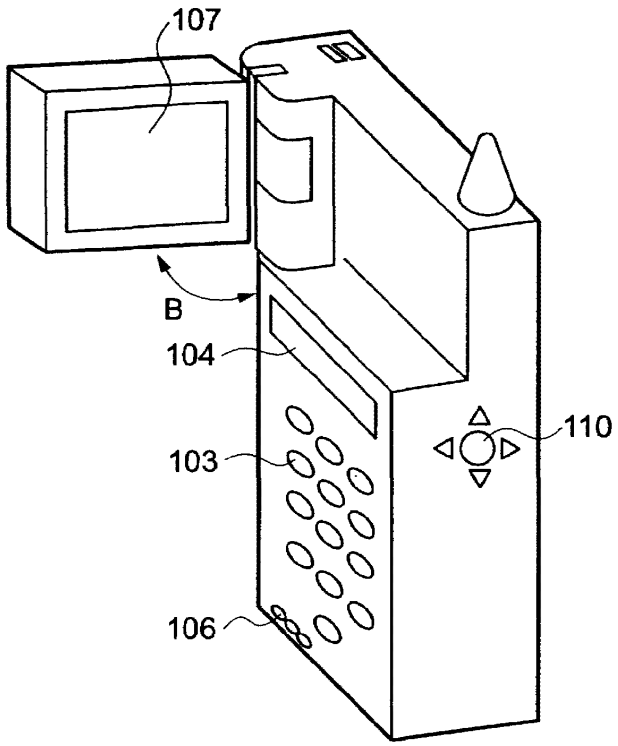


FIG.3

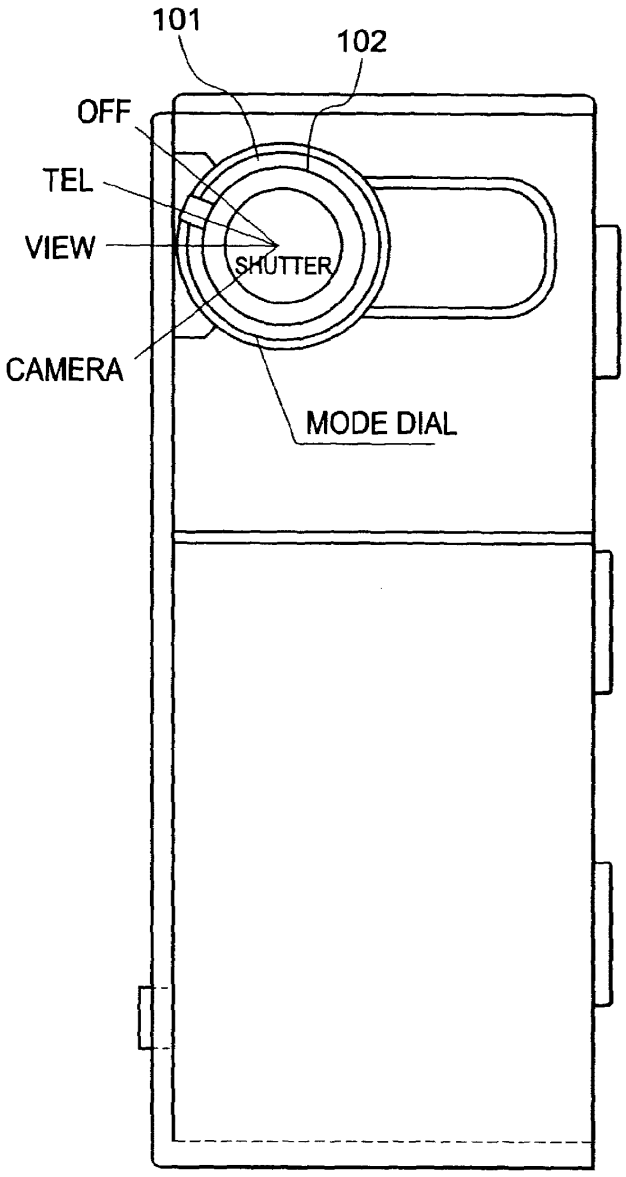
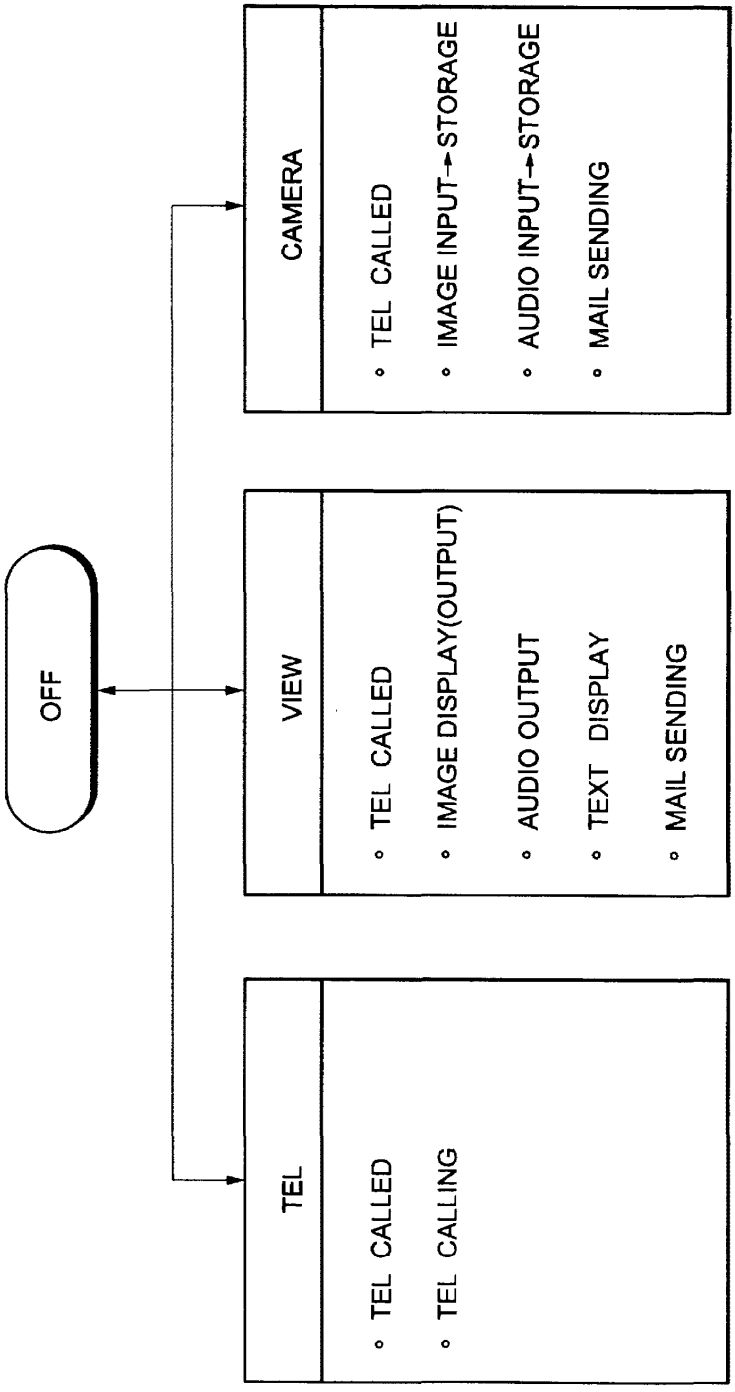


FIG.4



Ex.1002 / Page 1069 of 1311
APPLE INC.

FIG.5

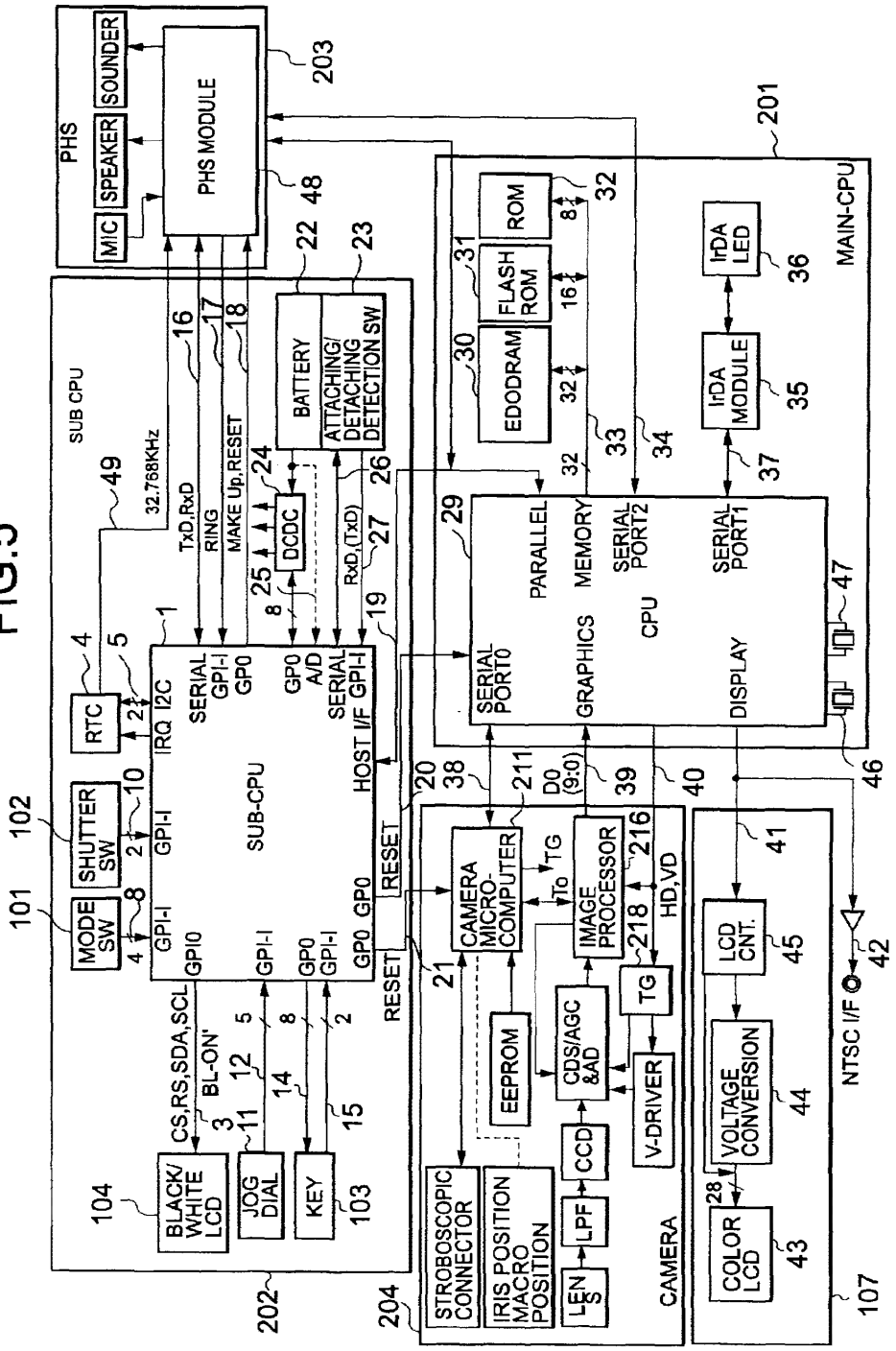

PHS
MIC
SPEAKER
SOUNDER
PHS MODULE
203
SUB CPU
SUB-CPU
32.768KHz
TxD,RxD
RING
MAKE Up,RESET
BATTERY
ATTACHING/ DETACHING DETECTION SW
DCDC
RxD,(TxD)
RTC
IRQ I2C
SERIAL GPI-I
GP0
GP0 A/D
HOST I/F
RESET
SHUTTER SW
MODE SW
GPI-I
GPI0
CS,RS,SDA,SCL
BL-ON'
BLACK/ WHITE LCD
JOG DIAL
KEY
103
104
101
102
202
204
MAIN-CPU
201
ROM
FLASH ROM
EDODRAM
PARALLEL
MEMORY
SERIAL PORT0
SERIAL PORT2
SERIAL PORT1
GRAPHICS
CPU
DISPLAY
IrDA LED
IrDA MODULE
CAMERA MICRO-COMPUTER
IMAGE PROCESSOR
D0 (9:0)
HD,VD
TG
CDS/AGC &AD
V-DRIVER
CCD
LPF
LENS
EEPROM
STROBOSCOPIC CONNECTOR
IRIS POSITION MACRO POSITION
CAMERA
LCD CNT.
VOLTAGE CONVERSION
COLOR LCD
NTSC I/F
107

FIG.6

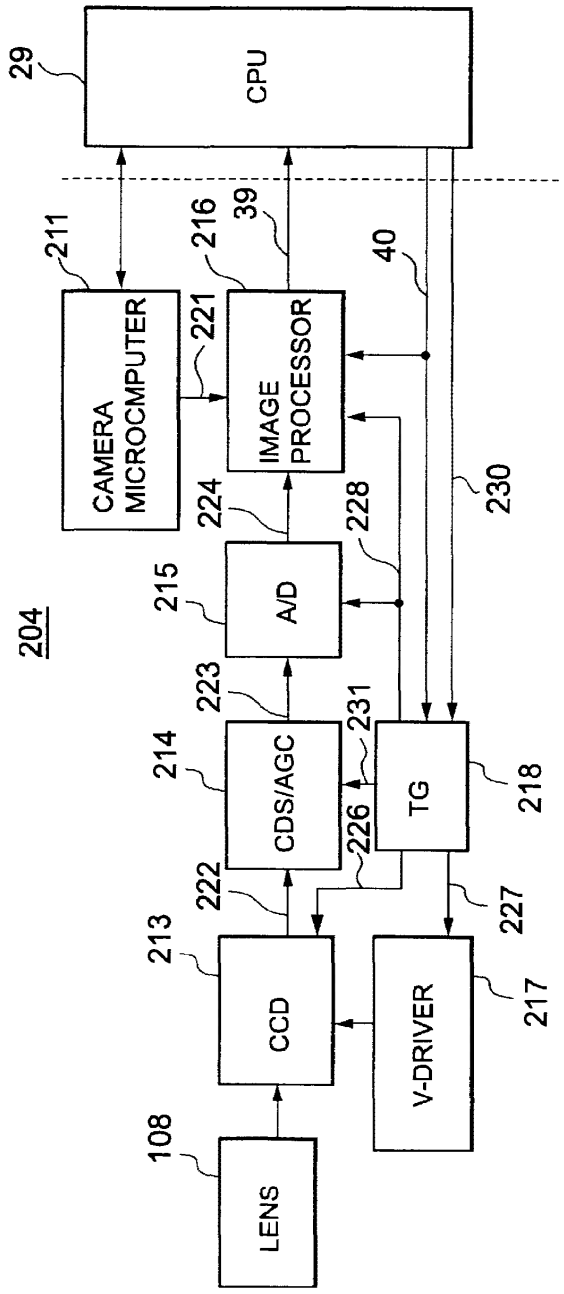

29
CPU
211
216
39
40
CAMERA MICROCMPUTER
221
IMAGE PROCESSOR
224
228
230
204
215
A/D
223
231
214
CDS/AGC
TG
218
226
222
227
213
CCD
V-DRIVER
217
108
LENS

FIG.7

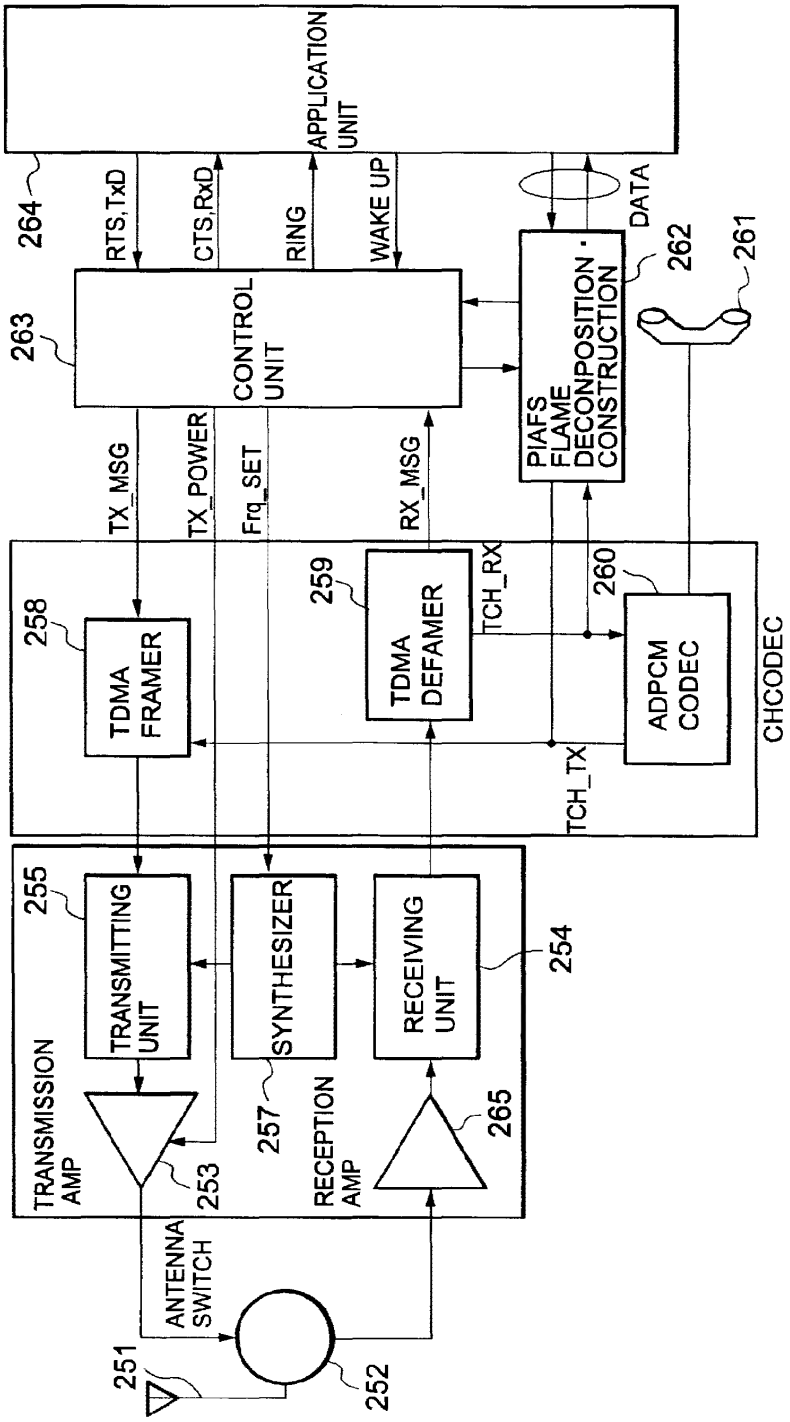

APPLICATION UNIT
264
RTS,TxD
CTS,RxD
RING
WAKE UP
DATA
263
CONTROL UNIT
262
261
PIAFS FLAME DECONPOSITION · CONSTRUCTION
TX_MSG
TX_POWER
Frq_SET
RX_MSG
258
TDMA FRAMER
259
TDMA DEFAMER
TCH_RX
260
ADPCM CODEC
CHCODEC
TCH_TX
255
TRANSMITTING UNIT
SYNTHESIZER
RECEIVING UNIT
254
TRANSMISSION AMP
253
257
RECEPTION AMP
265
ANTENNA SWITCH
251
252

FIG.8

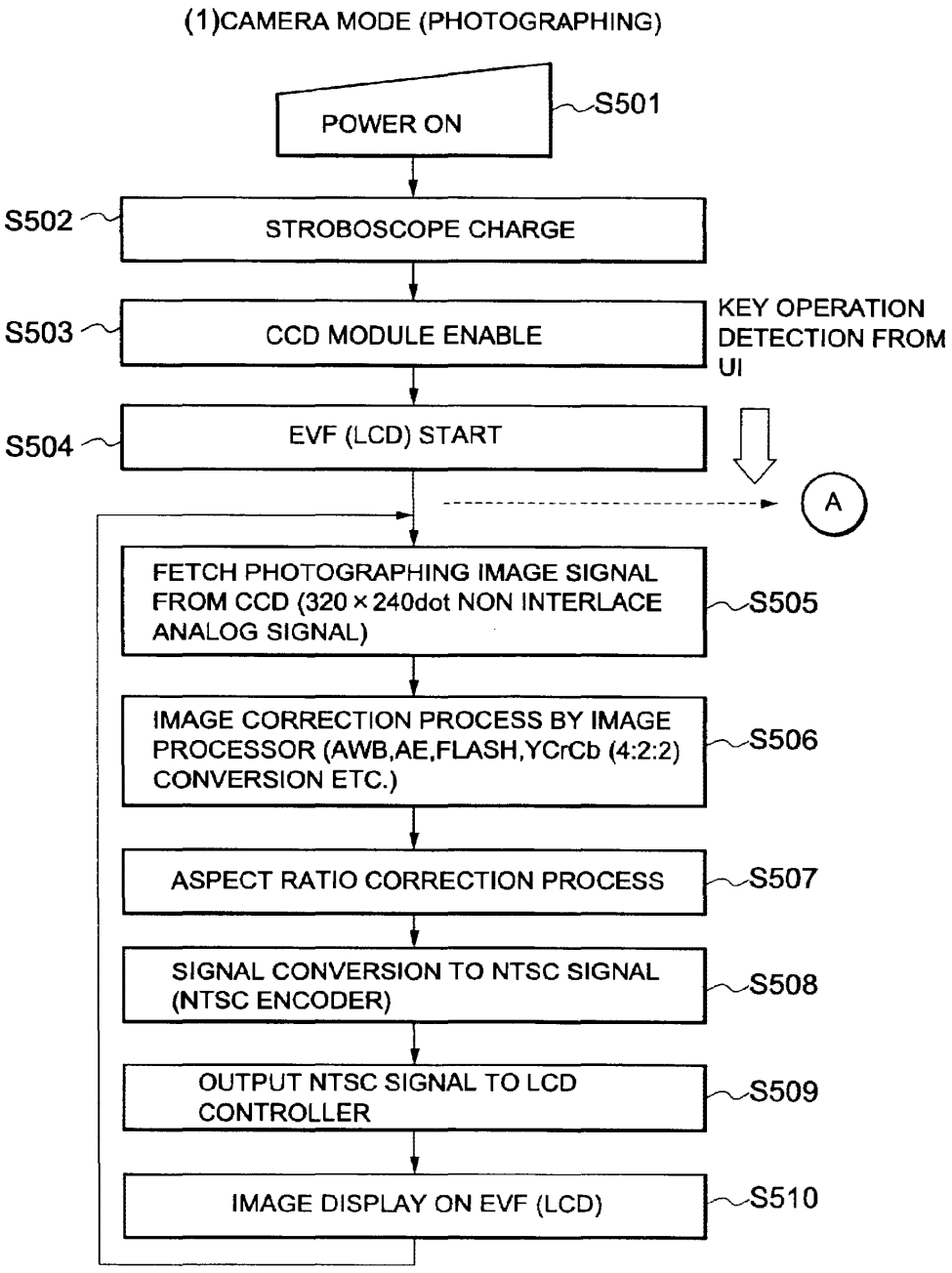

(1)CAMERA MODE (PHOTOGRAPHING)
POWER ON
S501
S502
STROBOSCOPE CHARGE
S503
CCD MODULE ENABLE
KEY OPERATION DETECTION FROM UI
S504
EVF (LCD) START
A
FETCH PHOTOGRAPHING IMAGE SIGNAL FROM CCD (320 × 240dot NON INTERLACE ANALOG SIGNAL)
S505
IMAGE CORRECTION PROCESS BY IMAGE PROCESSOR (AWB,AE,FLASH,YCrCb (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

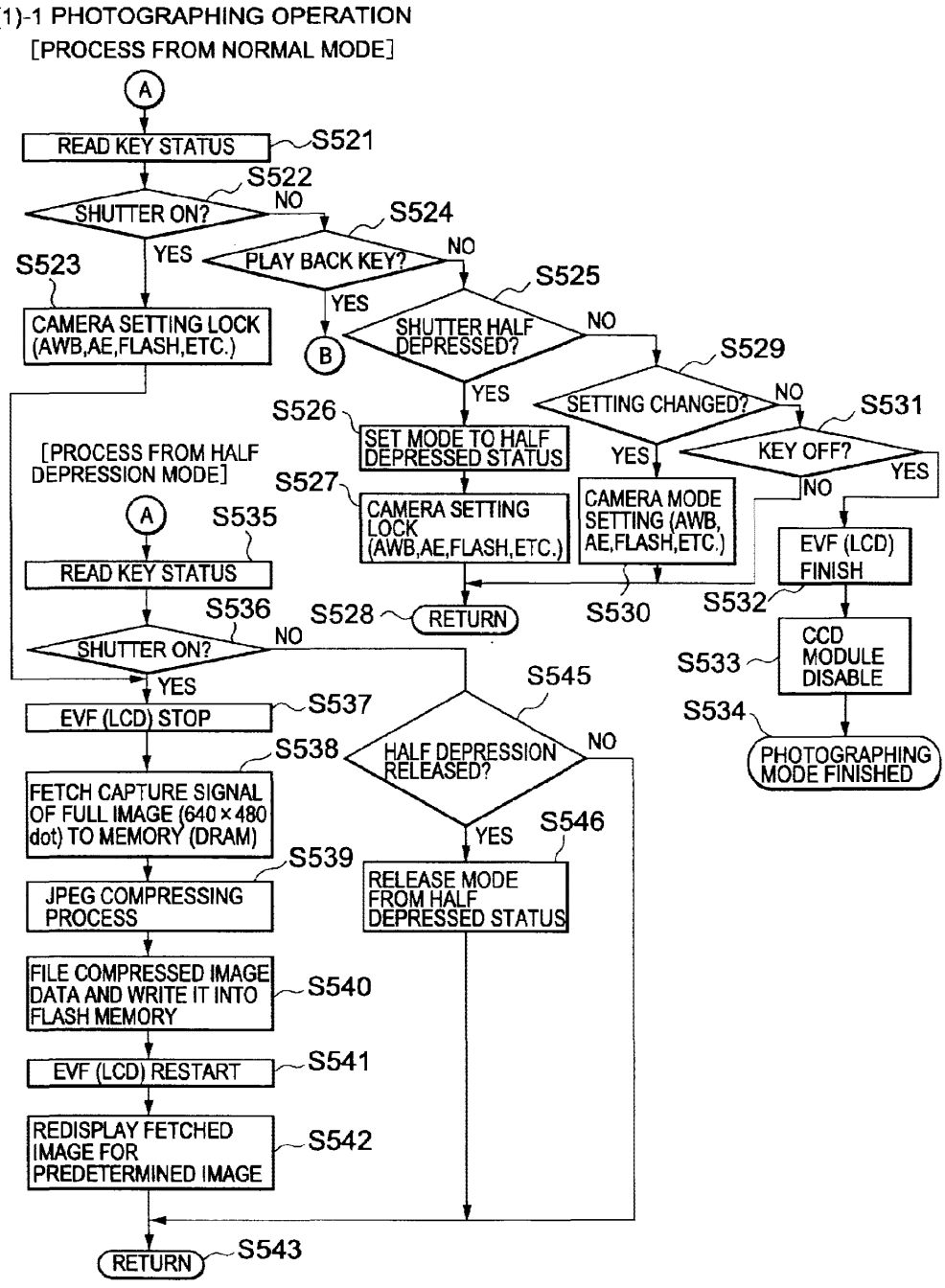

(1)-1 PHOTOGRAPHING OPERATION
[PROCESS FROM NORMAL MODE]
A
READ KEY STATUS
S521
S522
SHUTTER ON?
NO
S524
PLAY BACK KEY?
NO
YES
S523
YES
S525
CAMERA SETTING LOCK (AWB,AE,FLASH,ETC.)
B
SHUTTER HALF DEPRESSED?
NO
S529
YES
SETTING CHANGED?
NO
S531
S526
SET MODE TO HALF DEPRESSED STATUS
YES
KEY OFF?
YES
[PROCESS 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
FETCH CAPTURE SIGNAL OF FULL IMAGE (640 × 480 dot) TO MEMORY (DRAM)
YES
S546
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

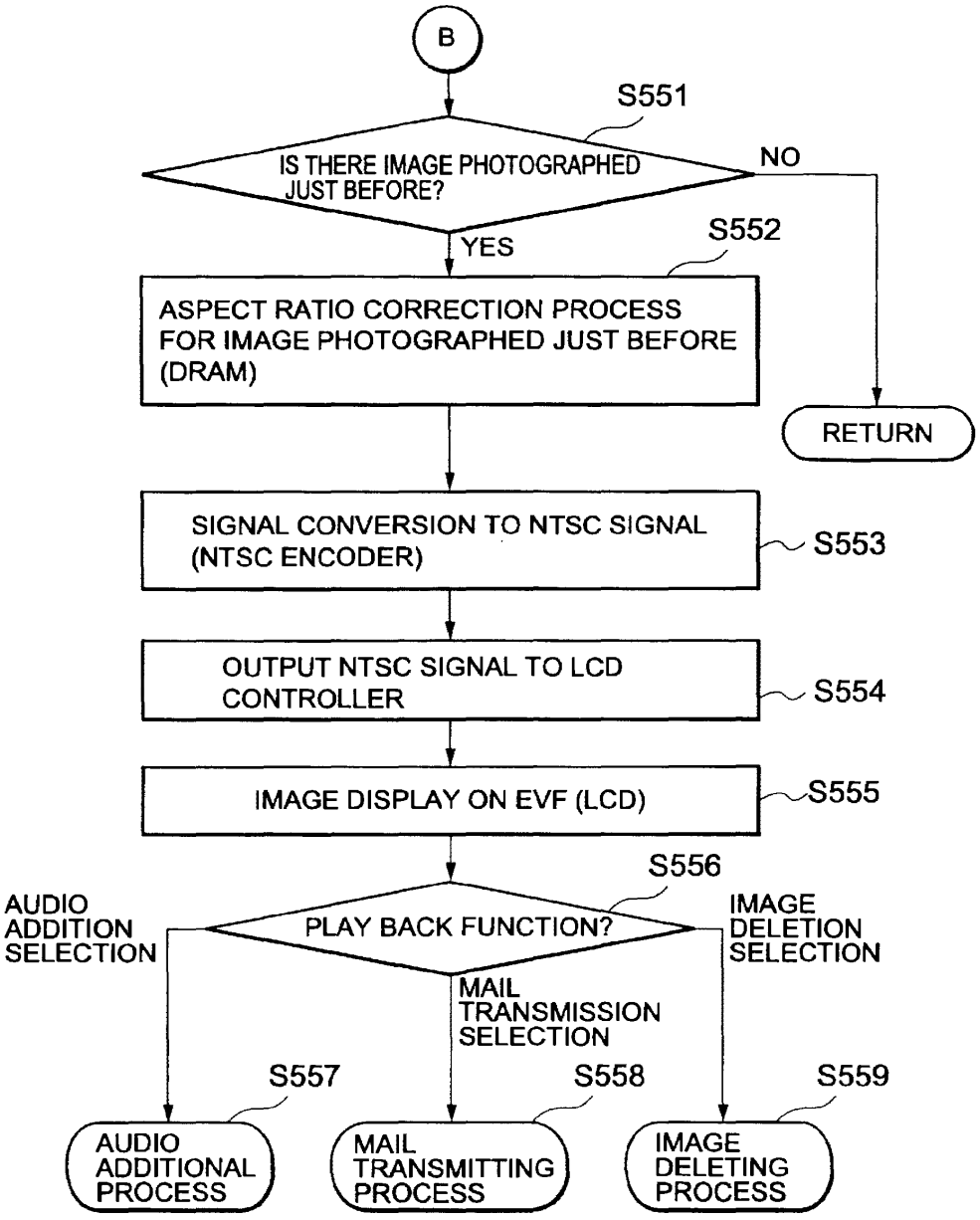


FIG.11

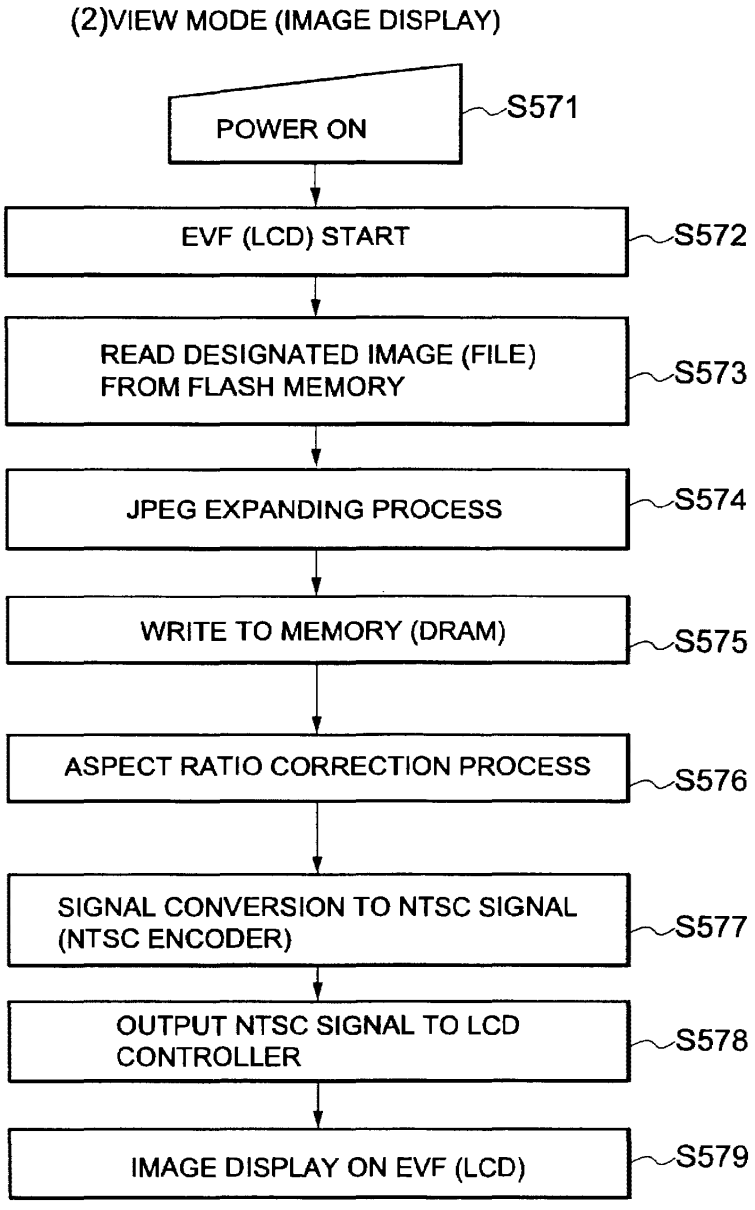
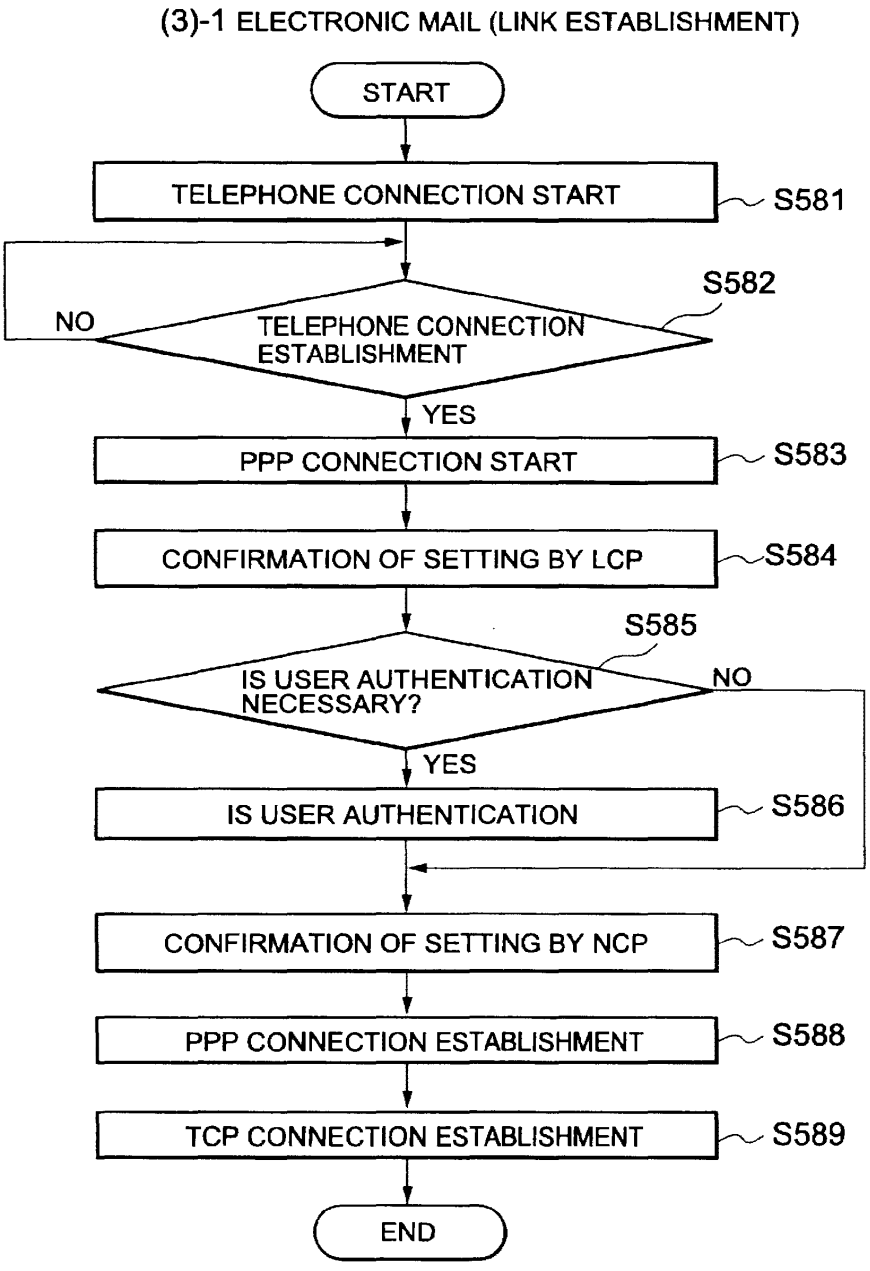

(2)VIEW MODE (IMAGE DISPLAY)
POWER ON
S571
EVF (LCD) START
S572
READ DESIGNATED IMAGE (FILE) FROM FLASH MEMORY
S573
JPEG EXPANDING PROCESS
S574
WRITE TO MEMORY (DRAM)
S575
ASPECT RATIO CORRECTION PROCESS
S576
SIGNAL CONVERSION TO NTSC SIGNAL (NTSC ENCODER)
S577
OUTPUT NTSC SIGNAL TO LCD CONTROLLER
S578
IMAGE DISPLAY ON EVF (LCD)
S579

FIG.12



Ex.1002 / Page 1077 of 1311
APPLE INC.

FIG.13

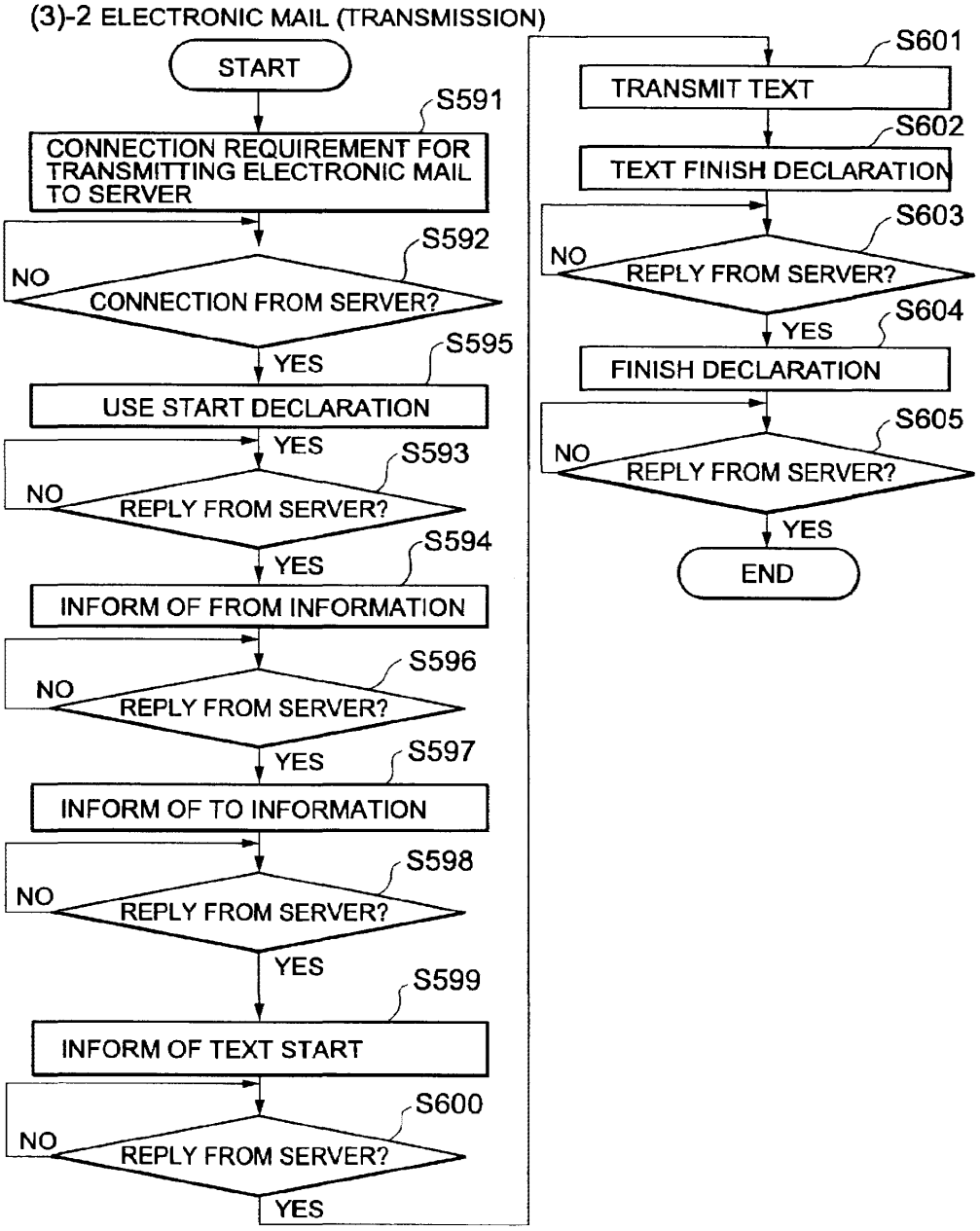

(3)-2 ELECTRONIC MAIL (TRANSMISSION)
START
S591
CONNECTION REQUIREMENT FOR TRANSMITTING ELECTRONIC MAIL TO SERVER
S592
NO
CONNECTION FROM SERVER?
YES
S595
USE START DECLARATION
YES
S593
NO
REPLY FROM SERVER?
YES
S594
INFORM OF FROM INFORMATION
S596
NO
REPLY FROM SERVER?
YES
S597
INFORM OF TO INFORMATION
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

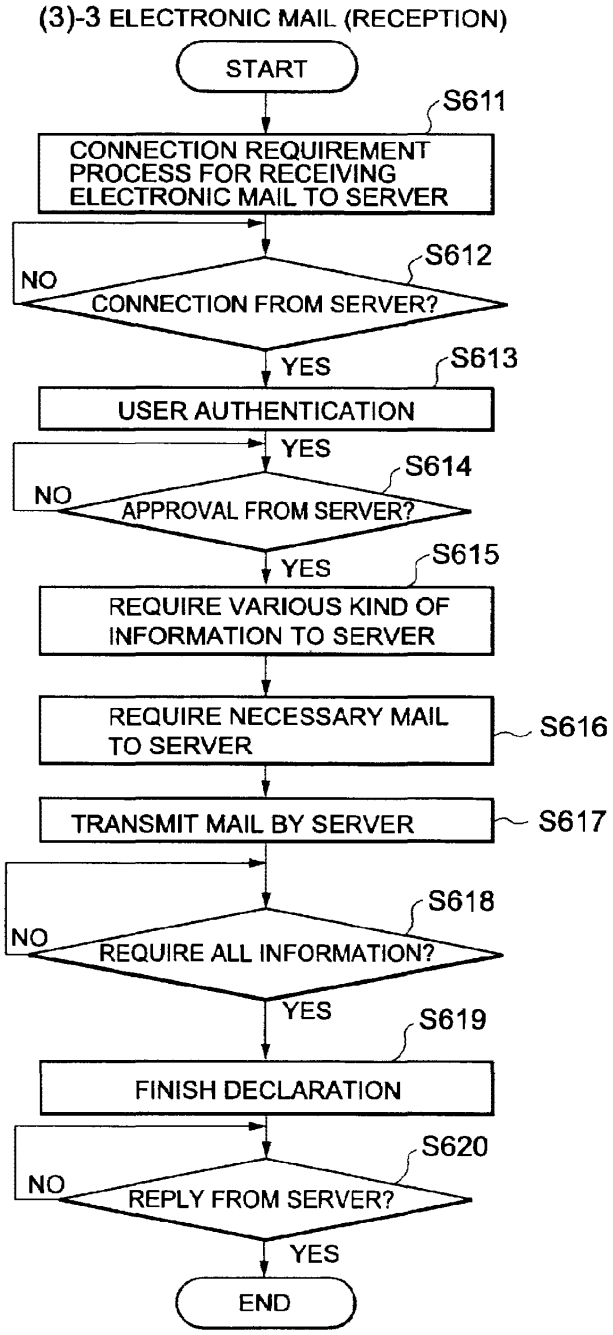

(3)-3 ELECTRONIC MAIL (RECEPTION)
START
S611
CONNECTION REQUIREMENT PROCESS FOR RECEIVING ELECTRONIC MAIL TO SERVER
S612
NO
CONNECTION FROM SERVER?
YES
S613
USER AUTHENTICATION
YES
S614
NO
APPROVAL FROM SERVER?
YES
S615
REQUIRE VARIOUS KIND OF INFORMATION TO SERVER
REQUIRE NECESSARY MAIL TO SERVER
S616
TRANSMIT MAIL BY SERVER
S617
S618
NO
REQUIRE ALL INFORMATION?
YES
S619
FINISH DECLARATION
S620
NO
REPLY FROM SERVER?
YES
END

FIG.15

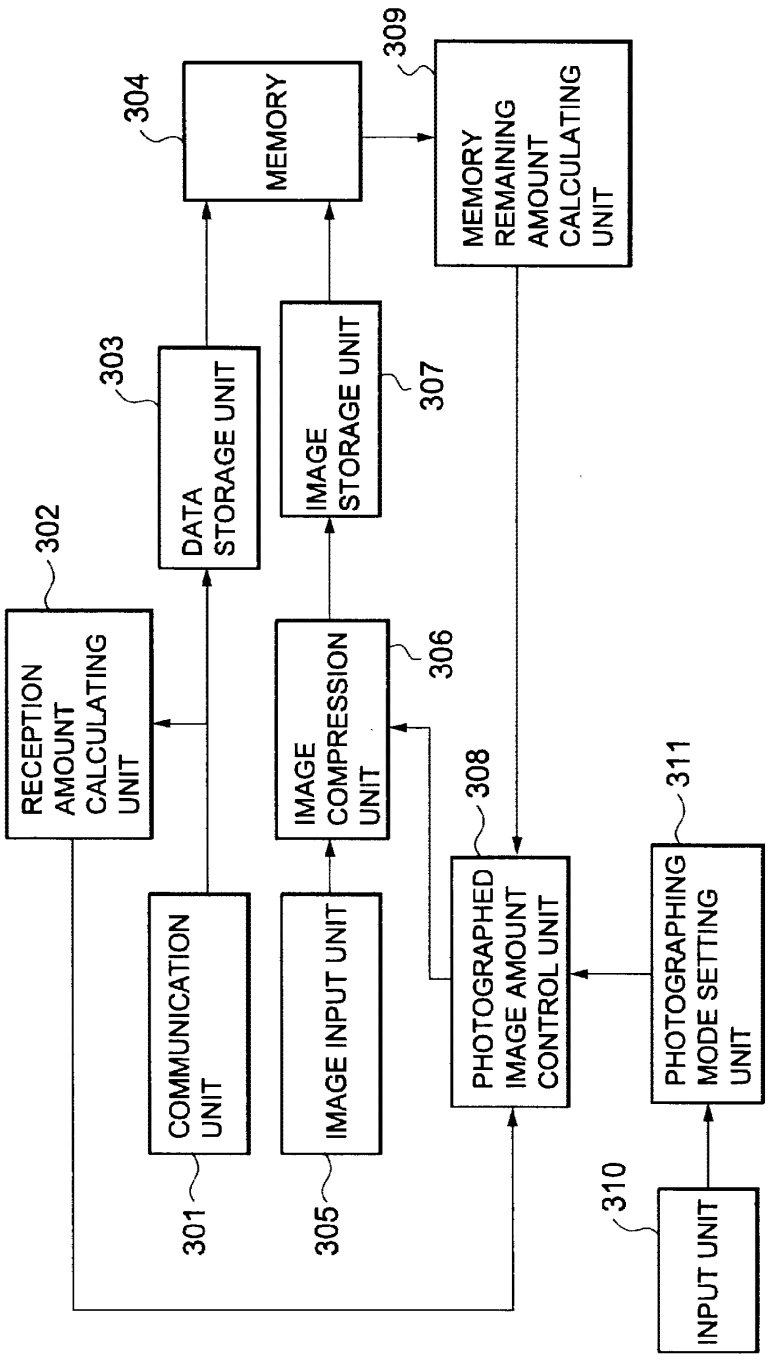

RECEPTION AMOUNT CALCULATING UNIT
302
DATA STORAGE UNIT
303
MEMORY
304
IMAGE STORAGE UNIT
307
MEMORY REMAINING AMOUNT CALCULATING UNIT
309
IMAGE COMPRESSION UNIT
306
PHOTOGRAPHED IMAGE AMOUNT CONTROL UNIT
308
PHOTOGRAPHING MODE SETTING UNIT
311
COMMUNICATION UNIT
301
IMAGE INPUT UNIT
305
INPUT UNIT
310

FIG.16

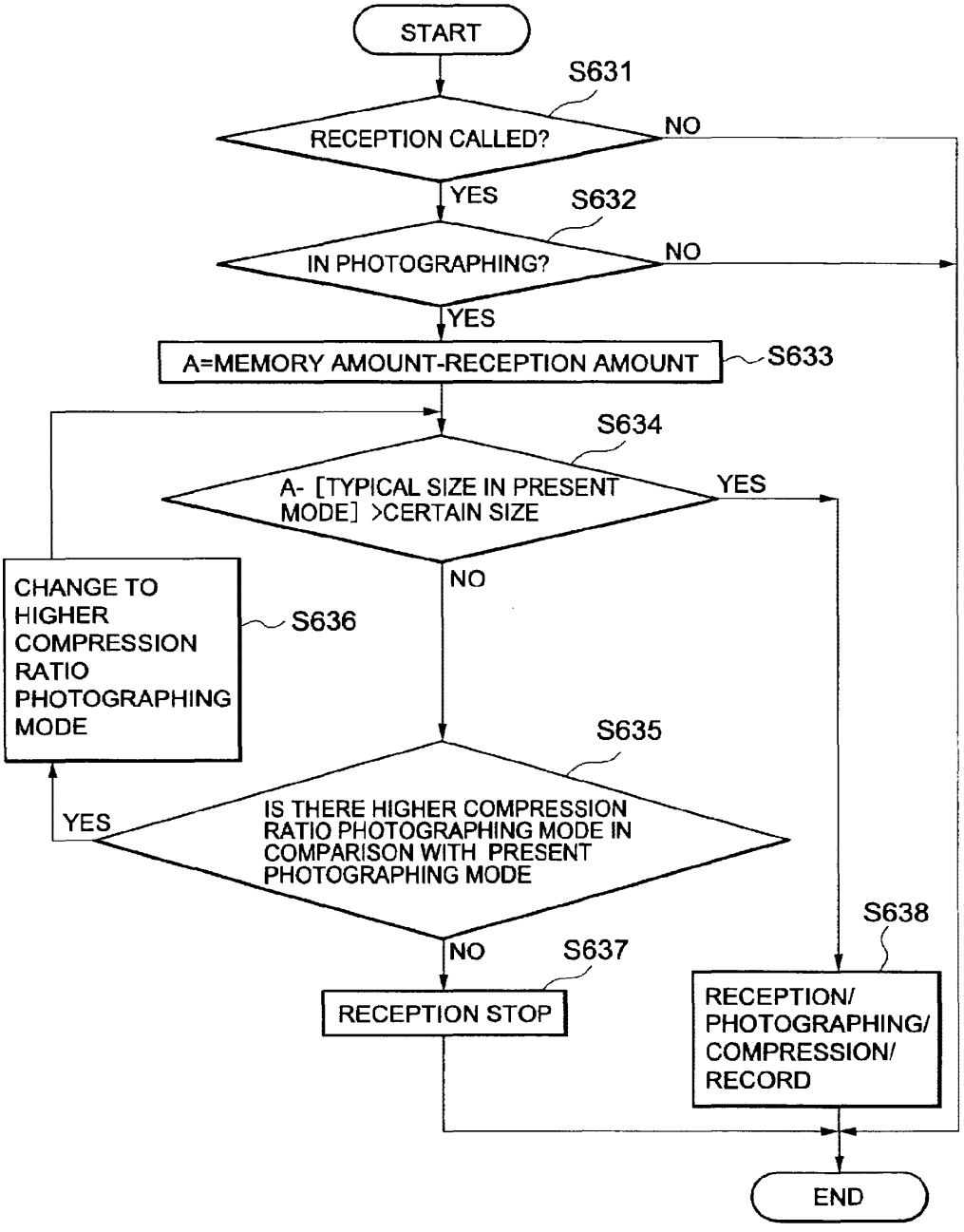
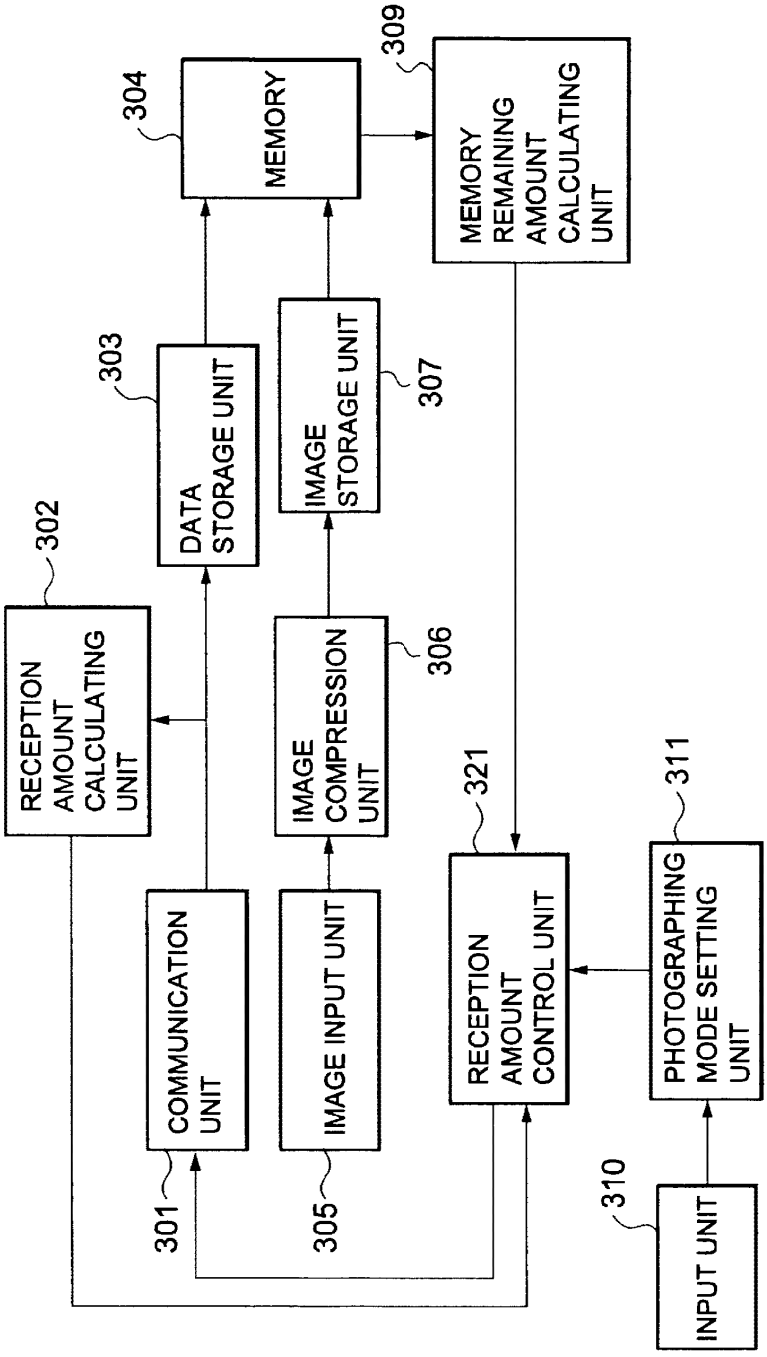

START
S631
RECEPTION CALLED?
NO
YES
S632
IN PHOTOGRAPHING?
NO
YES
A=MEMORY AMOUNT-RECEPTION AMOUNT
S633
S634
A- [TYPICAL SIZE IN PRESENT MODE] >CERTAIN SIZE
YES
NO
CHANGE TO HIGHER COMPRESSION RATIO PHOTOGRAPHING MODE
S636
S635
YES
IS THERE HIGHER COMPRESSION RATIO PHOTOGRAPHING MODE IN COMPARISON WITH PRESENT PHOTOGRAPHING MODE
S638
NO
S637
RECEPTION STOP
RECEPTION/ PHOTOGRAPHING/ COMPRESSION/ RECORD
END

FIG.17


MEMORY
304
309
MEMORY REMAINING AMOUNT CALCULATING UNIT
DATA STORAGE UNIT
303
IMAGE STORAGE UNIT
307
302
RECEPTION AMOUNT CALCULATING UNIT
IMAGE COMPRESSION UNIT
306
321
311
COMMUNICATION UNIT
IMAGE INPUT UNIT
RECEPTION AMOUNT CONTROL UNIT
PHOTOGRAPHING MODE SETTING UNIT
301
305
310
INPUT UNIT

Ex.1002 / Page 1083 of 1311
APPLE INC.

FIG.18

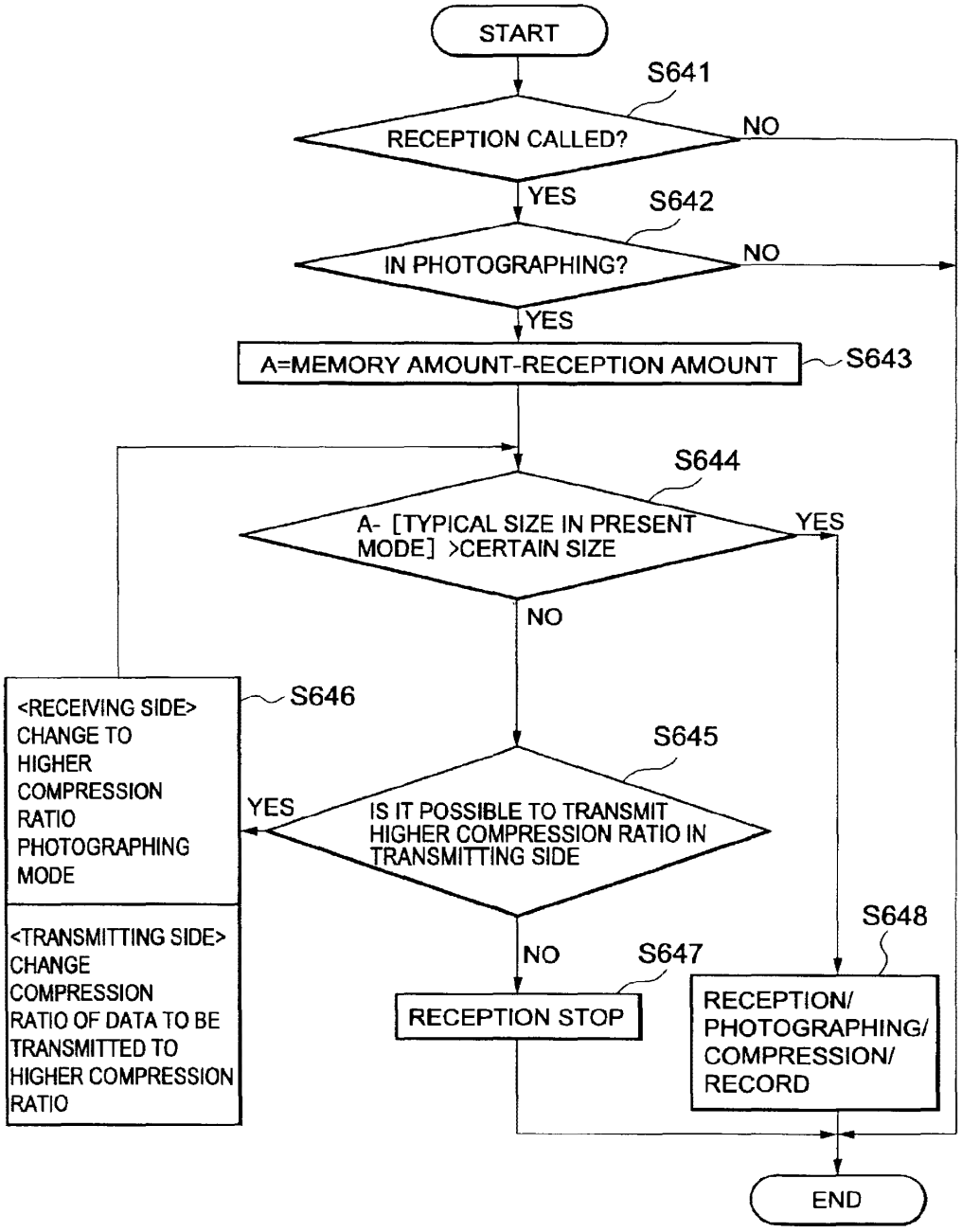


FIG.19

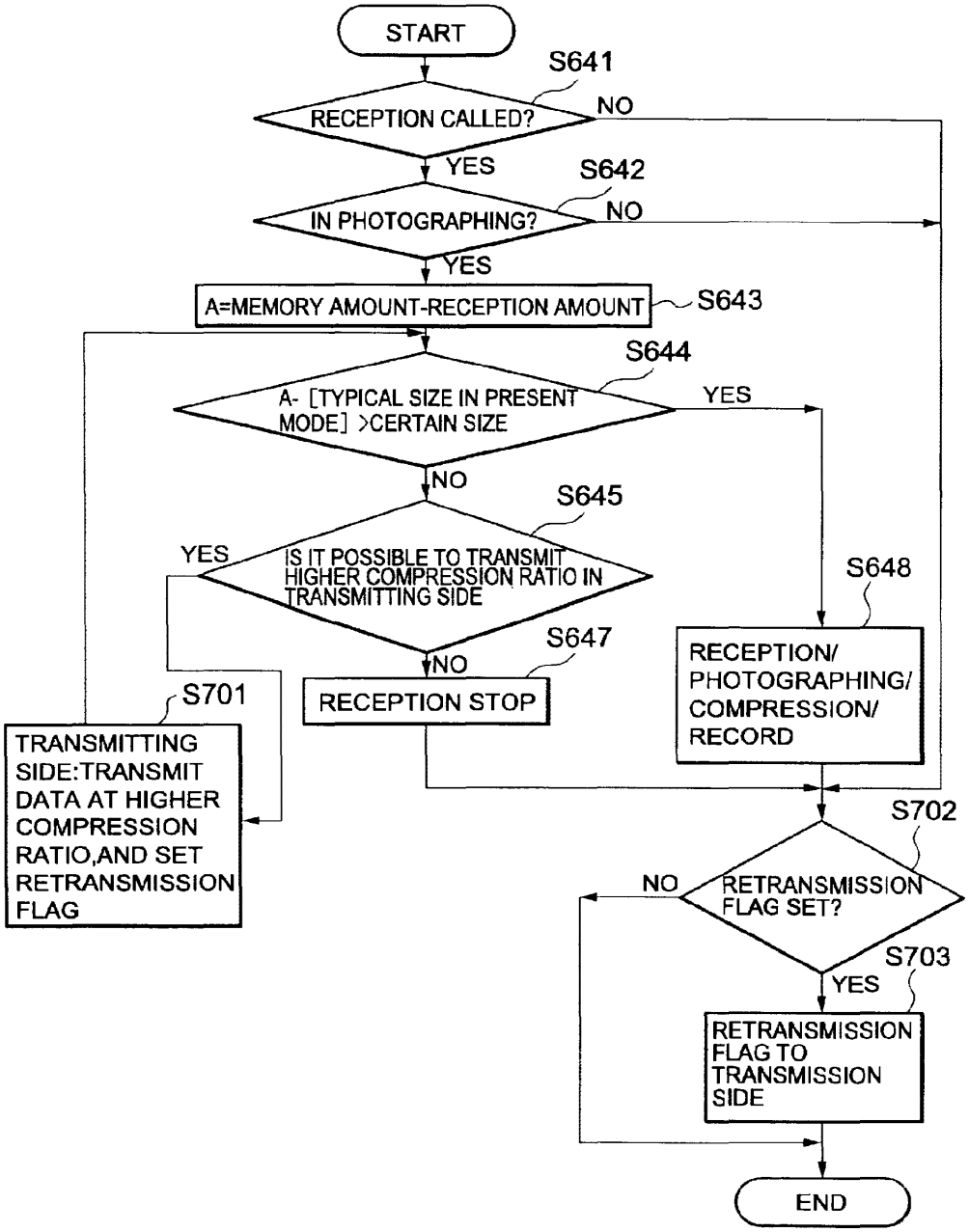

START
S641
RECEPTION CALLED?
NO
YES
S642
IN PHOTOGRAPHING?
NO
YES
A=MEMORY AMOUNT-RECEPTION AMOUNT
S643
S644
A- [TYPICAL SIZE IN PRESENT MODE] >CERTAIN SIZE
YES
NO
S645
YES
IS IT POSSIBLE TO TRANSMIT HIGHER COMPRESSION RATIO IN TRANSMITTING SIDE
S648
S647
NO
RECEPTION STOP
RECEPTION/ PHOTOGRAPHING/ COMPRESSION/ 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

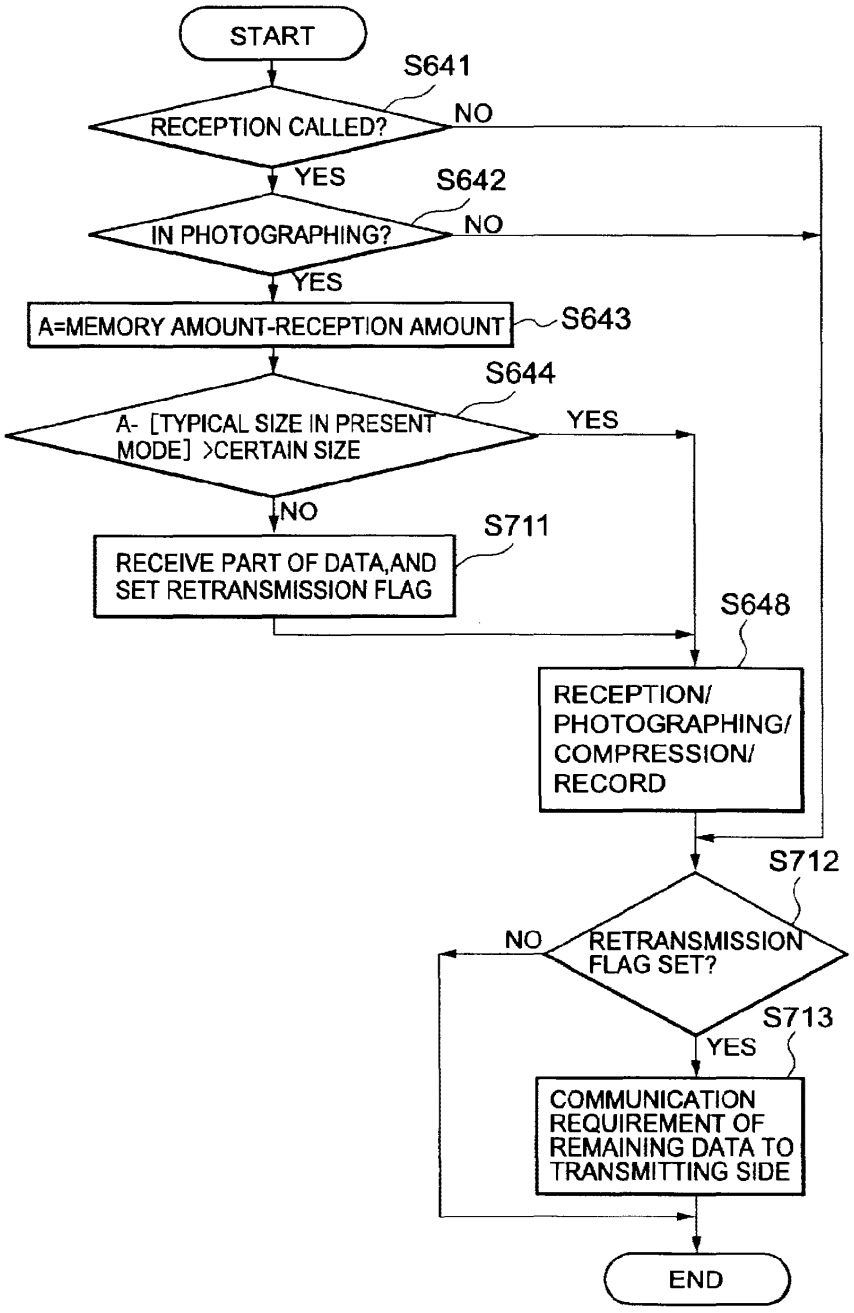

START
S641
RECEPTION CALLED?
NO
YES
S642
IN PHOTOGRAPHING?
NO
YES
A=MEMORY AMOUNT-RECEPTION AMOUNT
S643
S644
A- [TYPICAL SIZE IN PRESENT MODE] >CERTAIN SIZE
YES
NO
S711
RECEIVE PART OF DATA,AND SET RETRANSMISSION FLAG
S648
RECEPTION/ PHOTOGRAPHING/ COMPRESSION/ RECORD
S712
NO
RETRANSMISSION FLAG SET?
S713
YES
COMMUNICATION REQUIREMENT OF REMAINING DATA TO TRANSMITTING SIDE
END

FIG.21

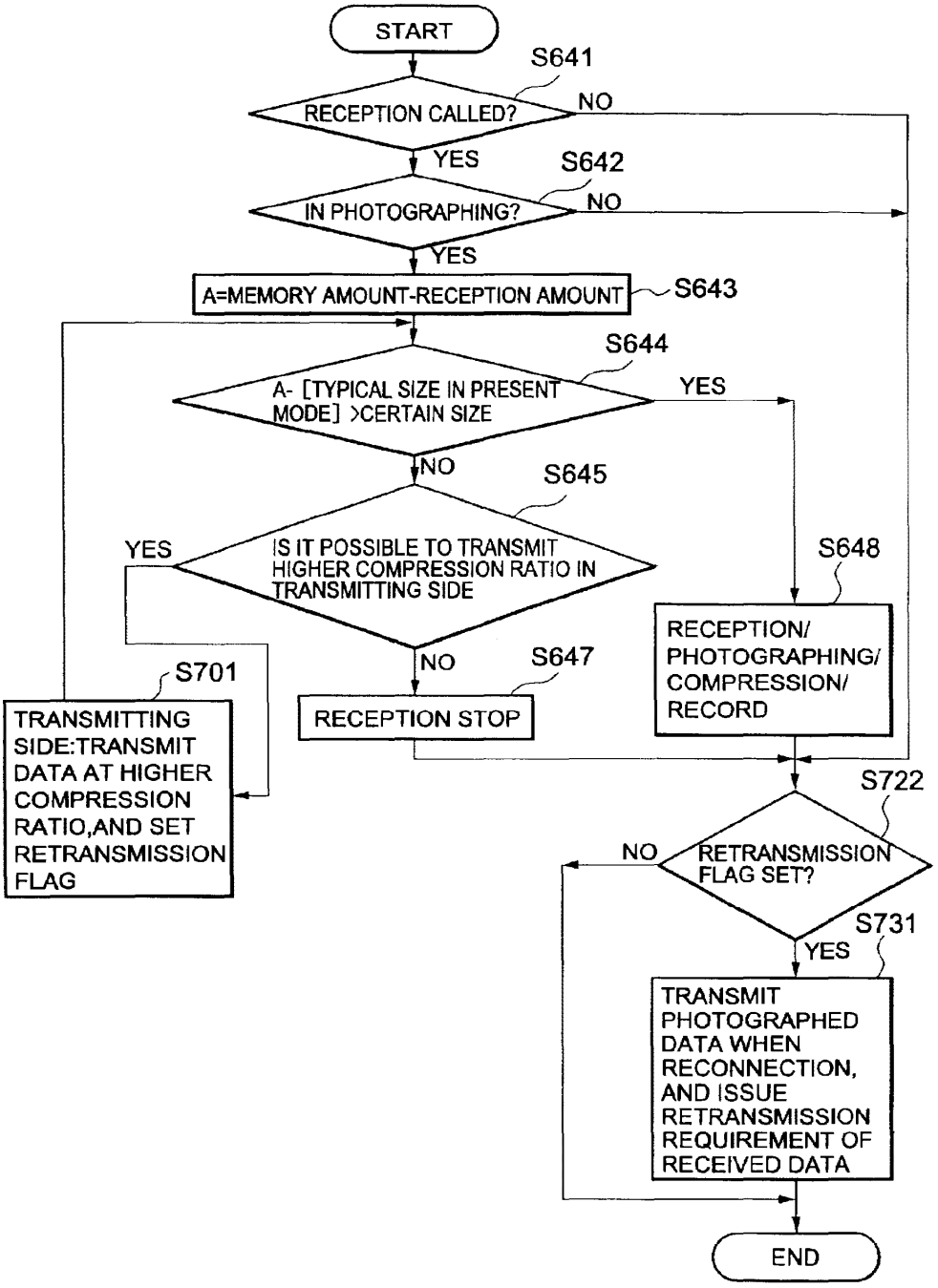
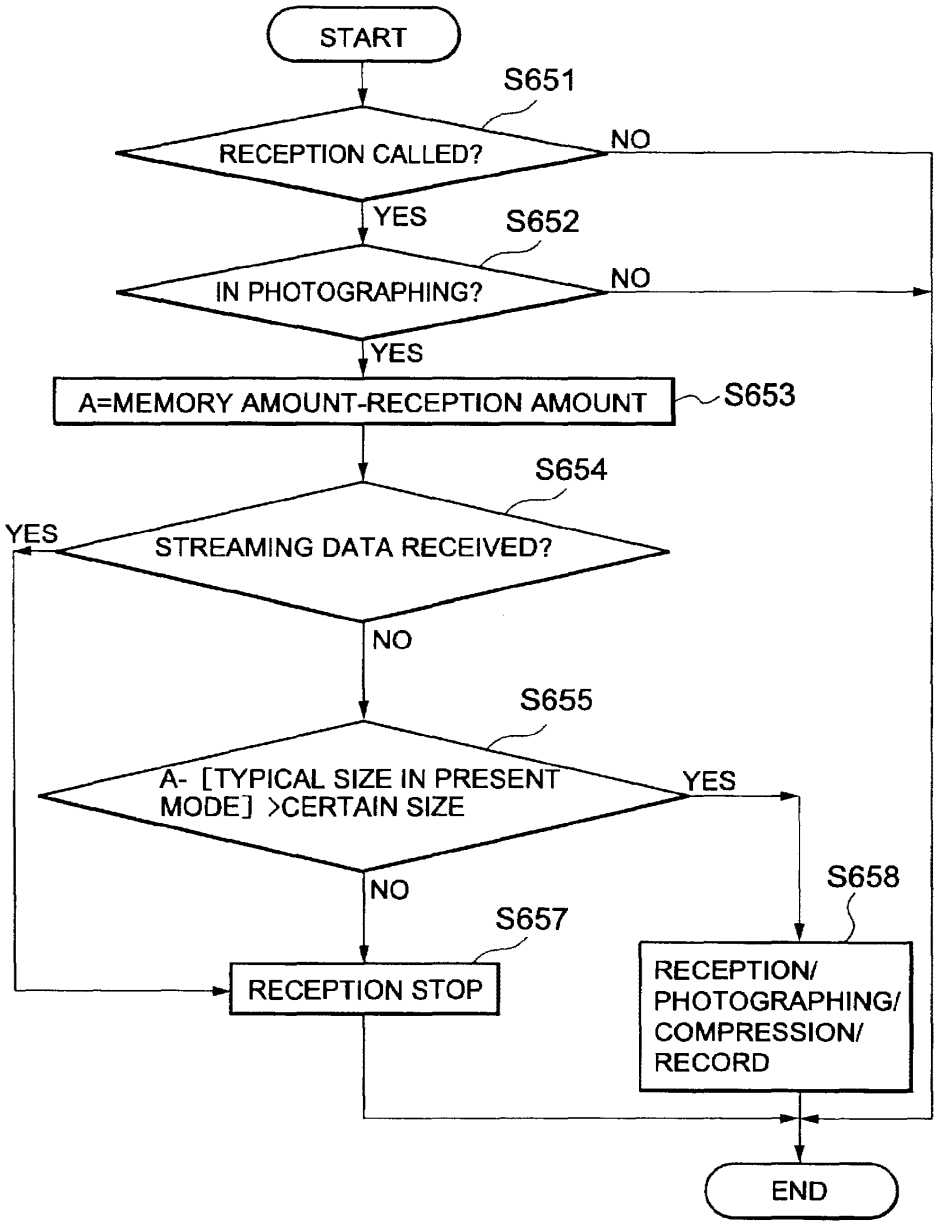

START
S641
RECEPTION CALLED?
NO
YES
S642
IN PHOTOGRAPHING?
NO
YES
A=MEMORY AMOUNT-RECEPTION AMOUNT
S643
S644
A- [TYPICAL SIZE IN PRESENT MODE] >CERTAIN SIZE
YES
NO
S645
YES
IS IT POSSIBLE TO TRANSMIT HIGHER COMPRESSION RATIO IN TRANSMITTING SIDE
S648
RECEPTION/ PHOTOGRAPHING/ COMPRESSION/ RECORD
NO
S647
RECEPTION STOP
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).

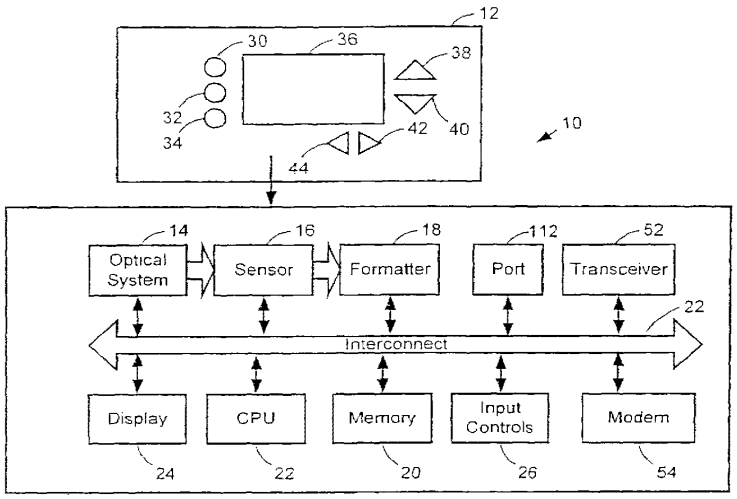
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, 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

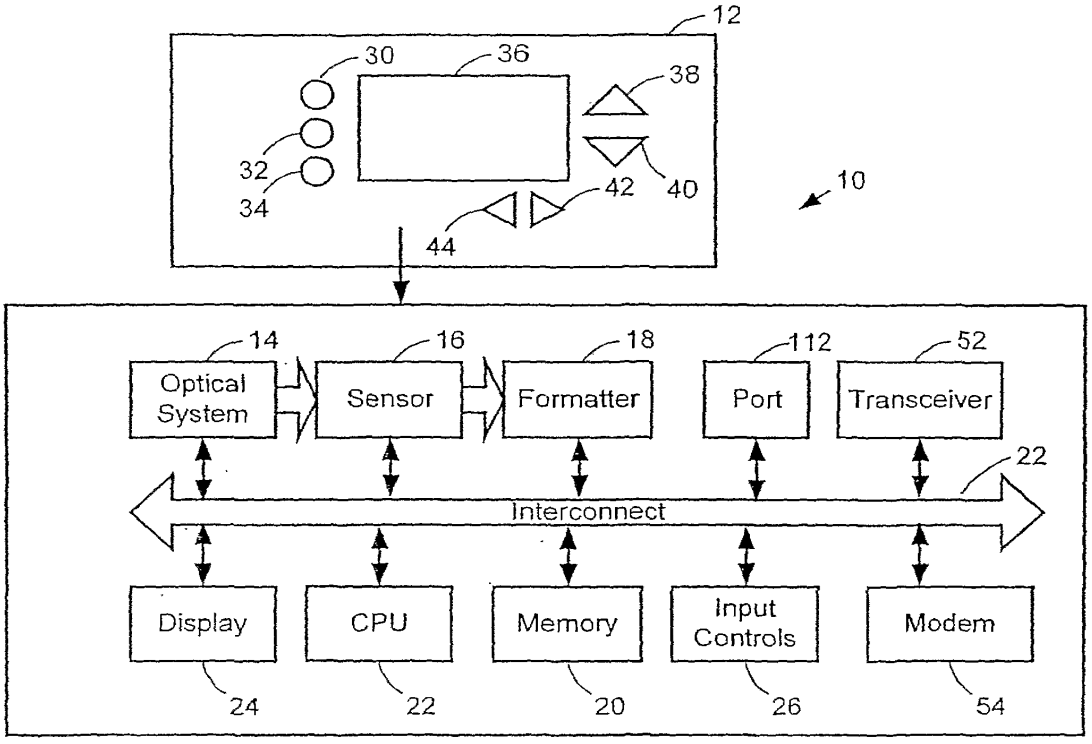

12
30
36
38
32
34
42
40
44
10
14
16
18
112
52
Optical System
Sensor
Formatter
Port
Transceiver
22
Interconnect
Display
CPU
Memory
Input Controls
Modem
24
22
20
26
54

Fig. 2

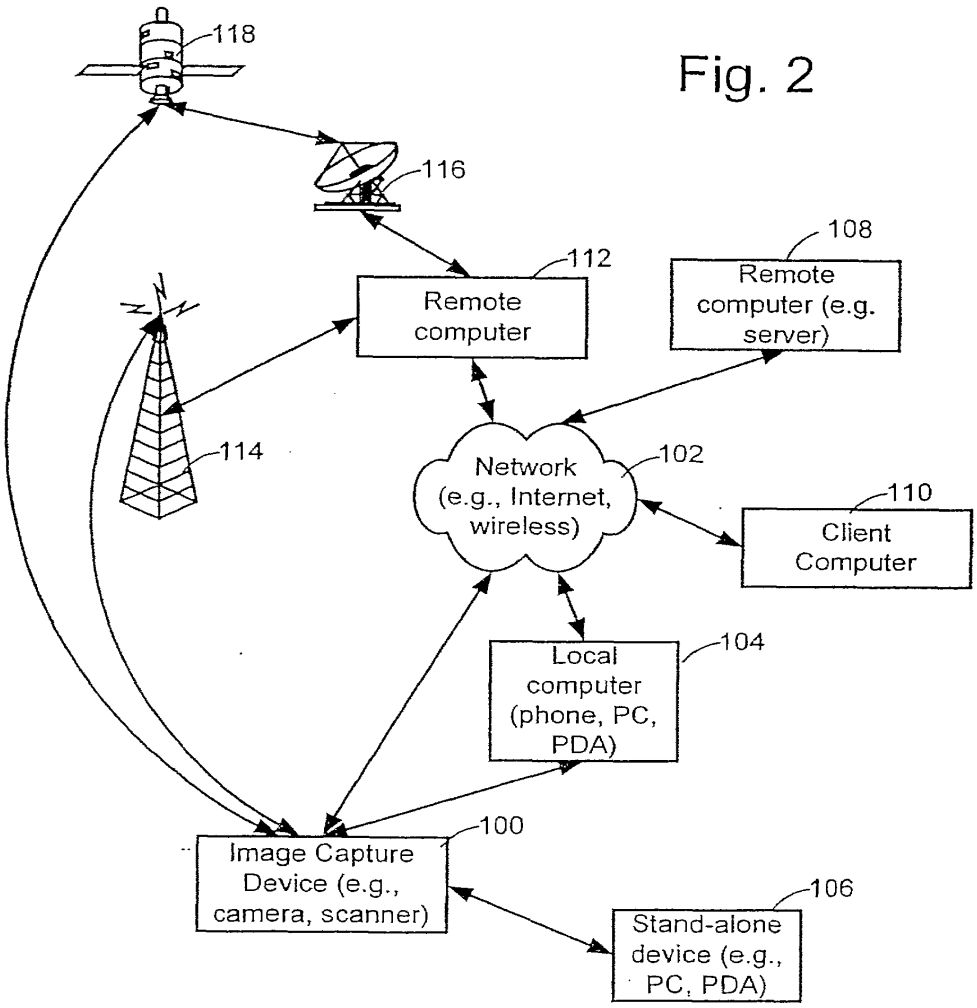

118
116
112
Remote computer
108
Remote computer (e.g. server)
114
Network (e.g., Internet, wireless)
102
110
Client Computer
Local computer (phone, PC, PDA)
104
Image Capture Device (e.g., camera, scanner)
100
106
Stand-alone device (e.g., PC, PDA)

Fig. 3

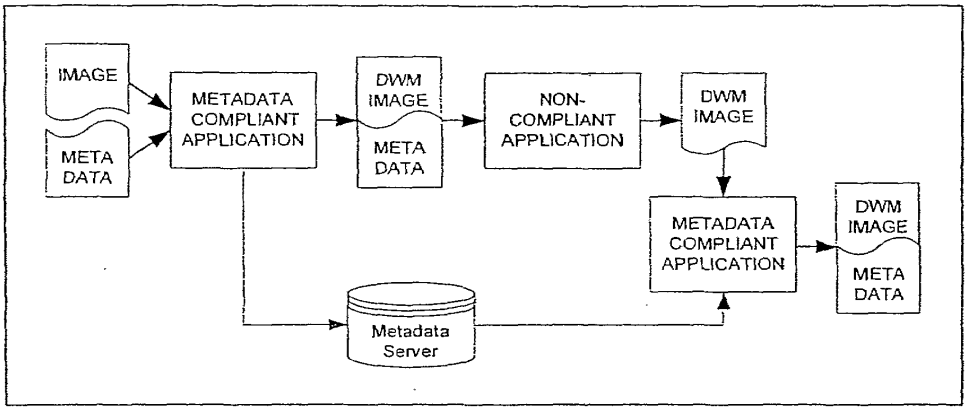
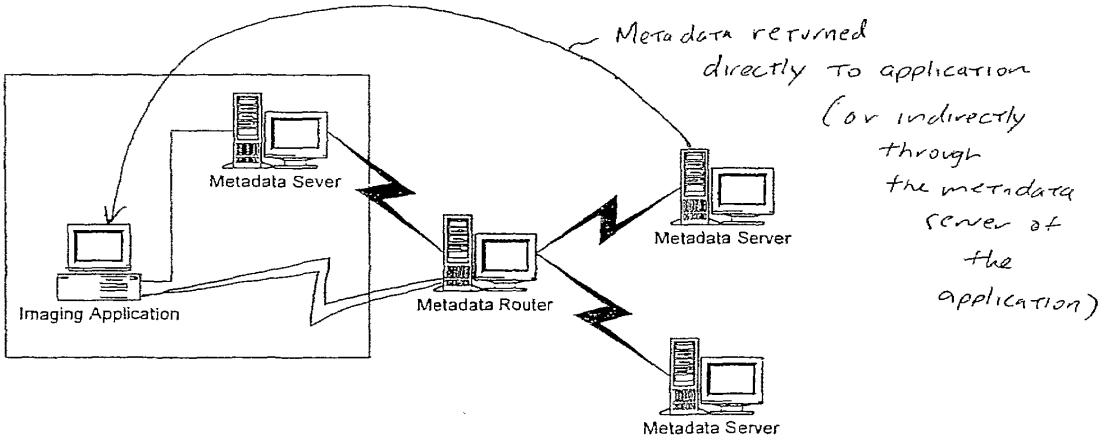

IMAGE
META DATA
METADATA COMPLIANT APPLICATION
DWM IMAGE
META DATA
NON-COMPLIANT APPLICATION
DWM IMAGE
METADATA COMPLIANT APPLICATION
DWM IMAGE
META DATA
Metadata Server

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).

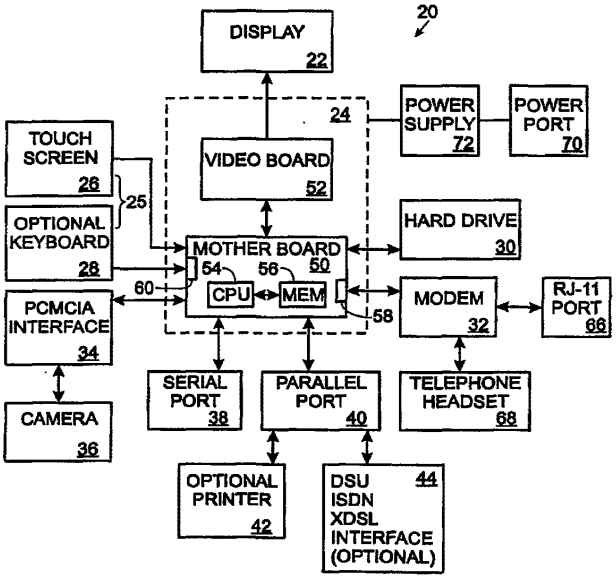
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: HAYHURST, Bill [US/US]; 25159 N.E. Butteville Road, Aurora, OR 97002 (US). WARD, Frederick, H. [US/US]; 13841 Tobiasson Road, Poway, CA 92604 (US). DABNEY, James, H. [US/US]; Suite B, 1366 Logan Avenue, Costa Mesa, CA 92626 (US).

(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.

Fig. 1

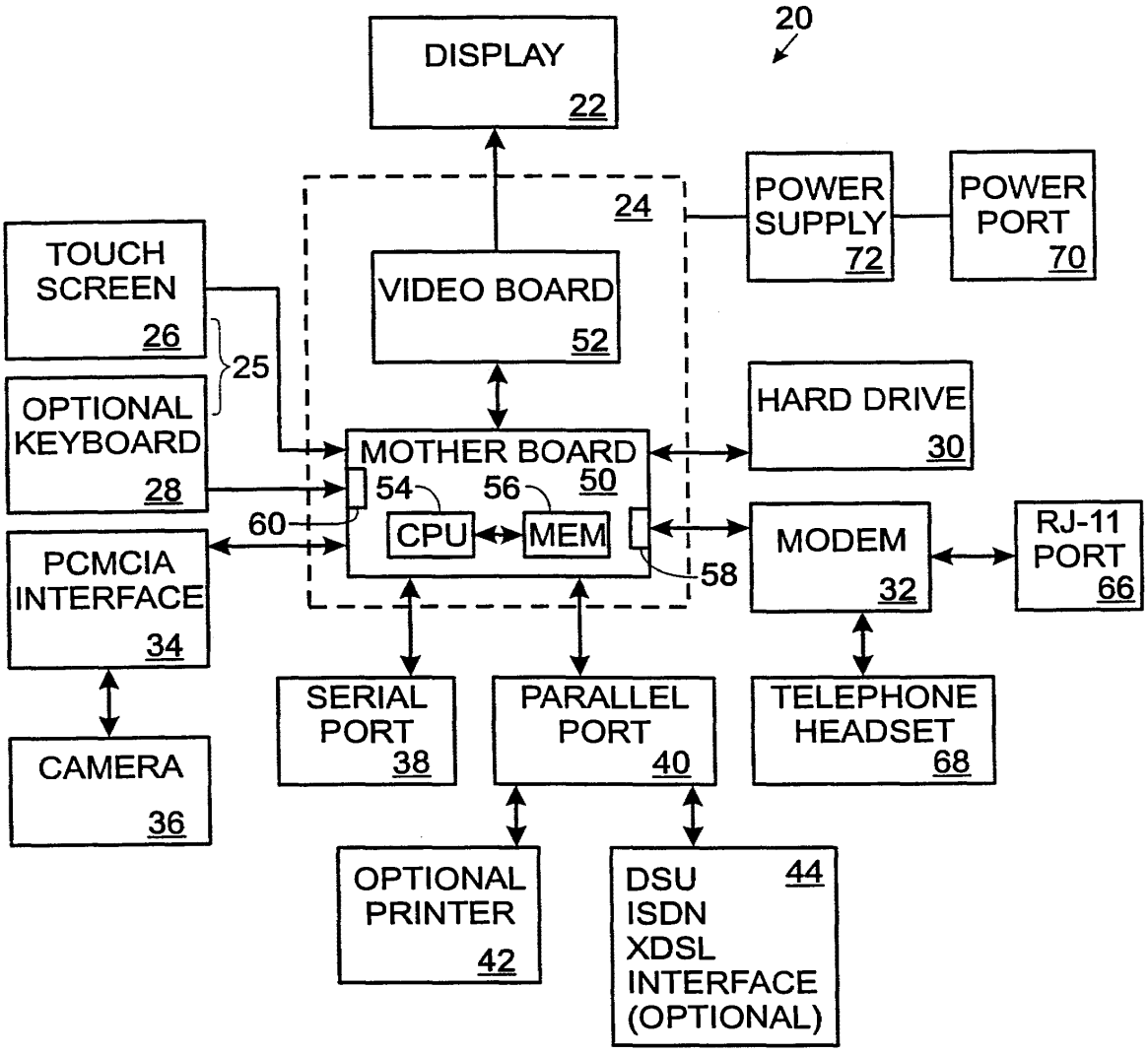

20
DISPLAY
22
24
POWER SUPPLY
72
POWER PORT
70
TOUCH SCREEN
26
25
VIDEO BOARD
52
OPTIONAL KEYBOARD
28
HARD DRIVE
30
MOTHER BOARD
50
54
56
CPU
MEM
60
58
PCMCIA INTERFACE
34
MODEM
32
RJ-11 PORT
66
SERIAL PORT
38
PARALLEL PORT
40
TELEPHONE HEADSET
68
CAMERA
36
OPTIONAL PRINTER
42
DSU
ISDN
XDSL
INTERFACE
(OPTIONAL)
44

Fig. 2

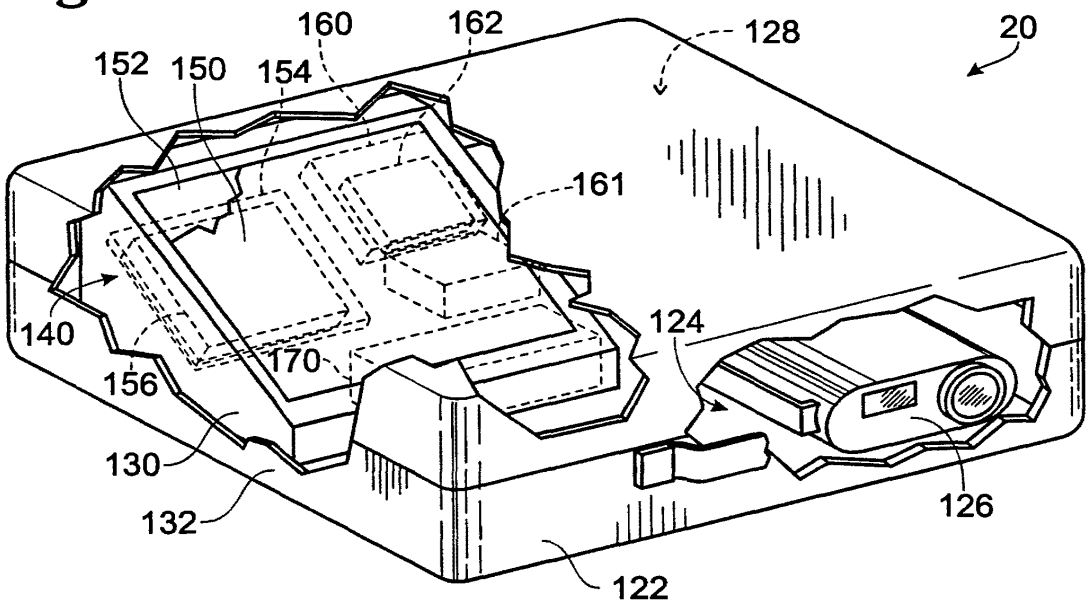

160
162
128
20
152
150
154
161
140
124
170
156
130
126
132
122

Fig. 6

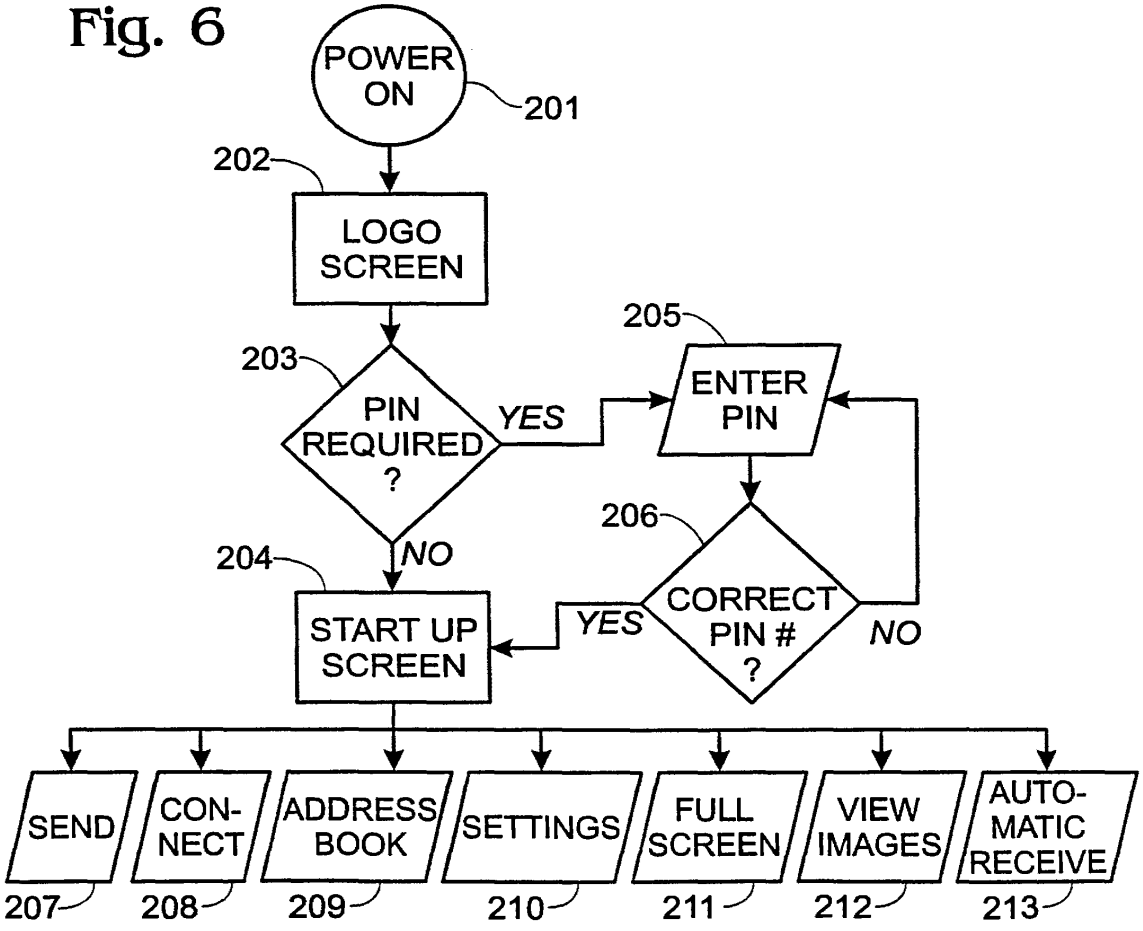

POWER ON
201
202
LOGO SCREEN
205
203
PIN REQUIRED ?
YES
ENTER PIN
206
NO
204
CORRECT PIN # ?
YES
NO
START UP SCREEN
SEND
CON-NECT
ADDRESS BOOK
SETTINGS
FULL SCREEN
VIEW IMAGES
AUTO-MATIC RECEIVE
207
208
209
210
211
212
213

Fig. 3

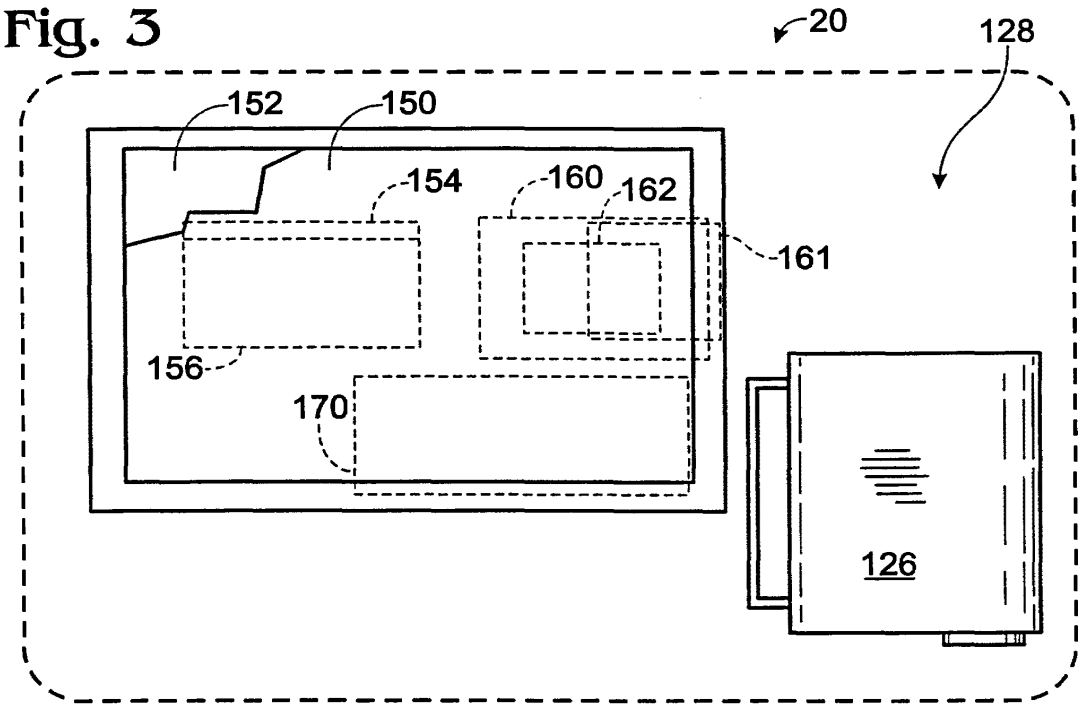


Fig. 4

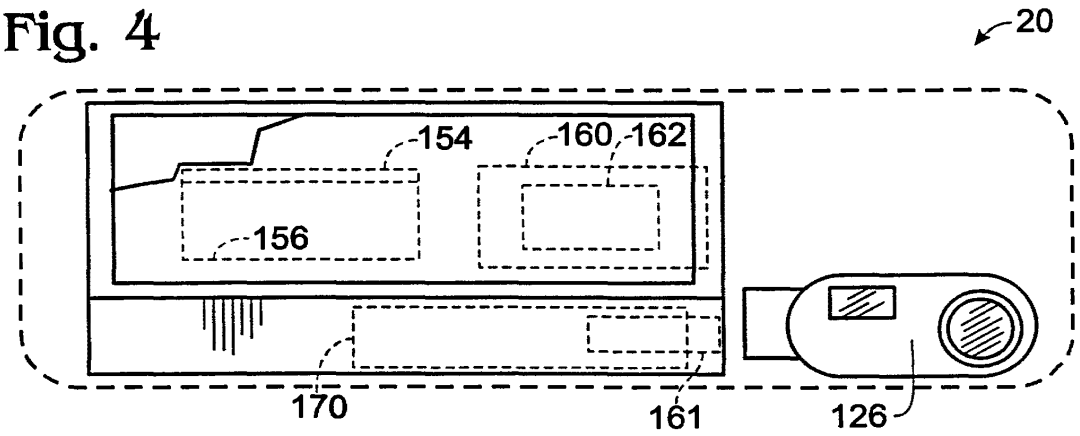


Fig. 5

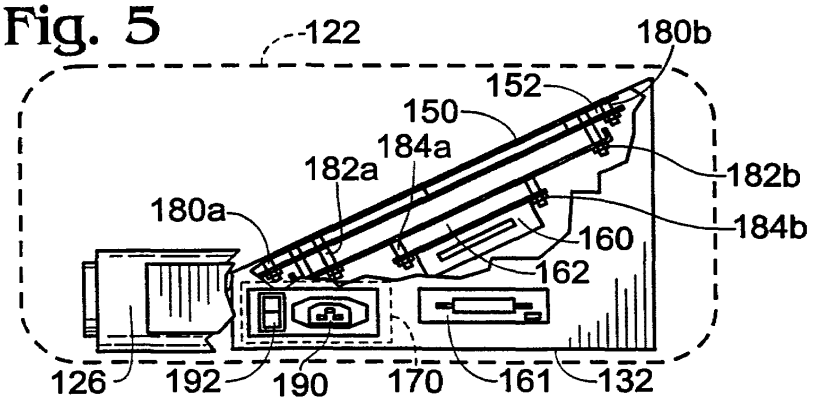


Fig. 8

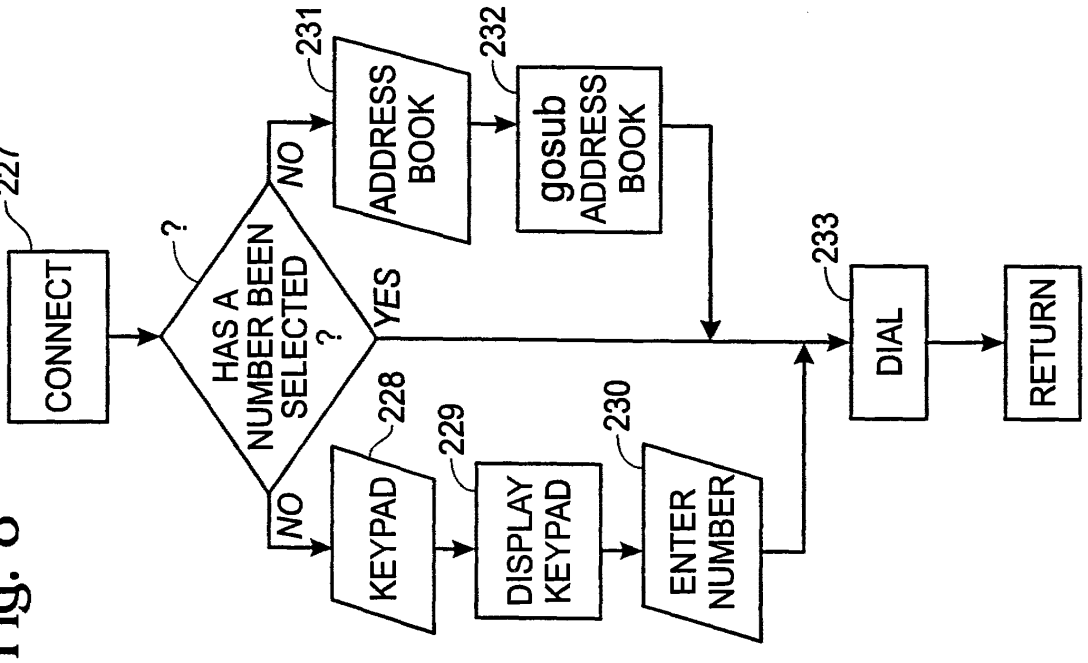

227
CONNECT
HAS A NUMBER BEEN SELECTED ?
YES
NO
231
ADDRESS BOOK
232
gosub ADDRESS BOOK
228
KEYPAD
229
DISPLAY KEYPAD
230
ENTER NUMBER
233
DIAL
RETURN

Fig. 7

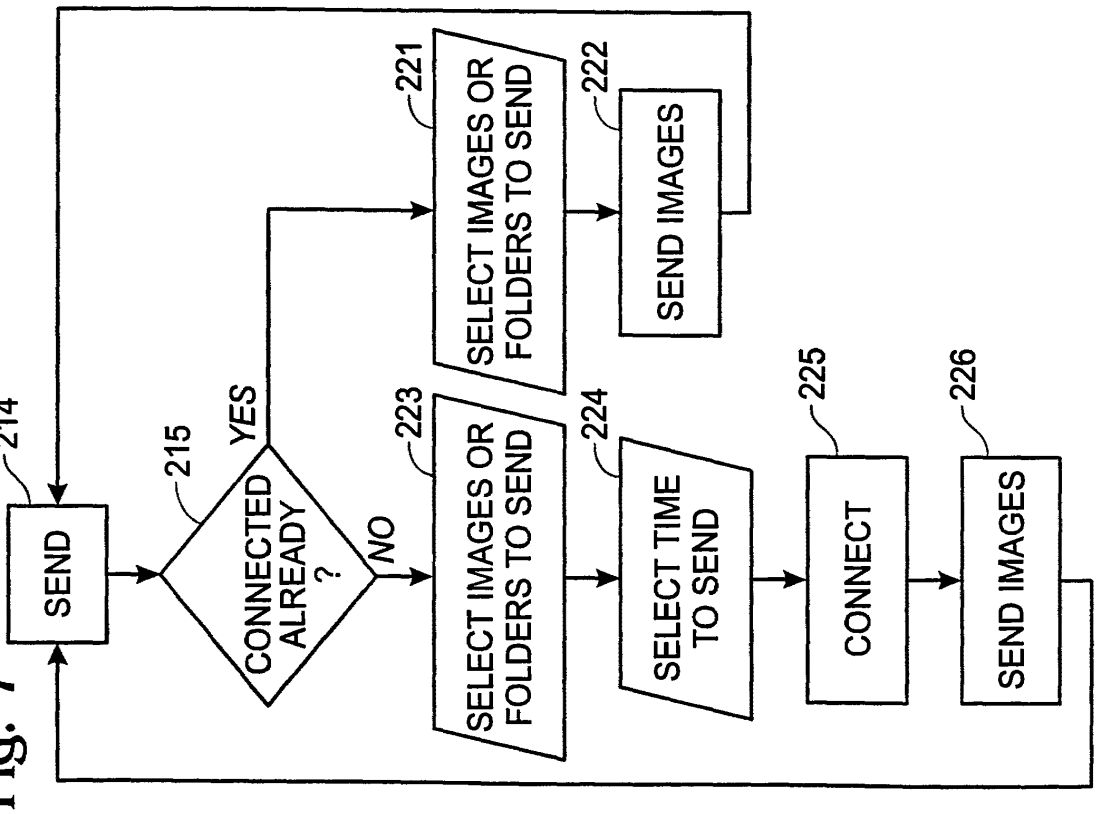

214
SEND
215
CONNECTED ALREADY ?
YES
NO
221
SELECT IMAGES OR FOLDERS TO SEND
222
SEND IMAGES
223
SELECT IMAGES OR FOLDERS TO SEND
224
SELECT TIME TO SEND
225
CONNECT
226
SEND IMAGES

Fig. 9

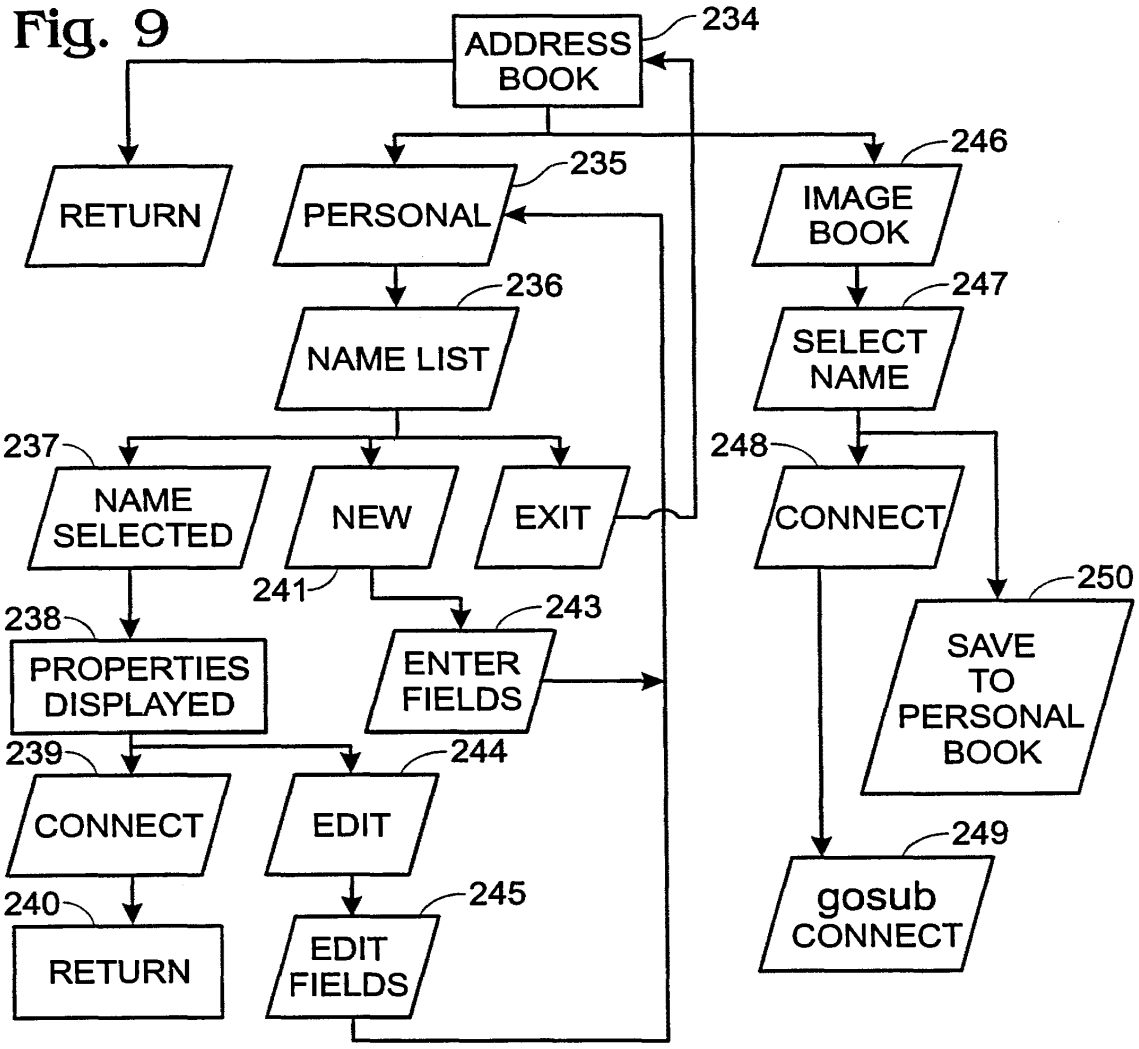

ADDRESS BOOK
234
RETURN
PERSONAL
235
IMAGE BOOK
246
NAME LIST
236
SELECT NAME
247
237
NAME SELECTED
NEW
EXIT
248
CONNECT
241
243
250
238
PROPERTIES DISPLAYED
ENTER FIELDS
SAVE TO PERSONAL BOOK
239
244
CONNECT
EDIT
249
240
245
RETURN
EDIT FIELDS
gosub CONNECT

Fig. 14

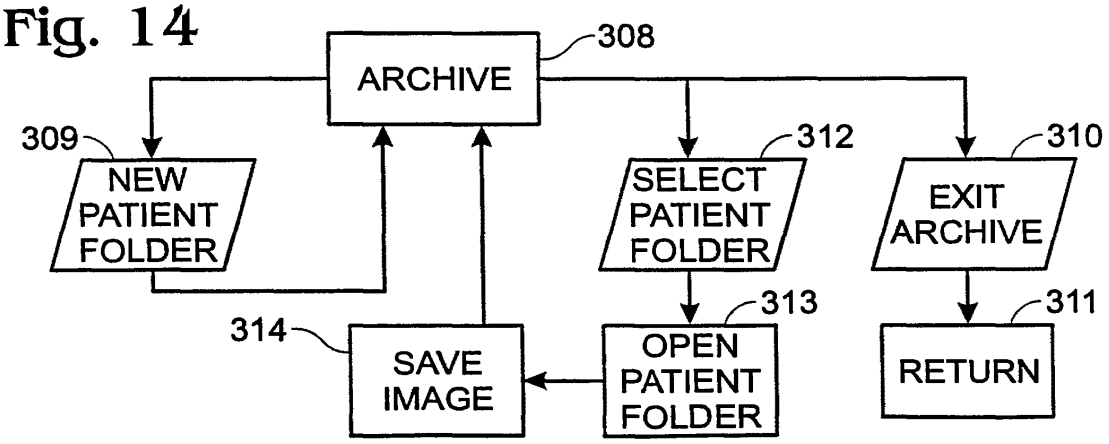

ARCHIVE
308
309
NEW PATIENT FOLDER
312
SELECT PATIENT FOLDER
310
EXIT ARCHIVE
313
314
SAVE IMAGE
OPEN PATIENT FOLDER
311
RETURN

Fig. 10

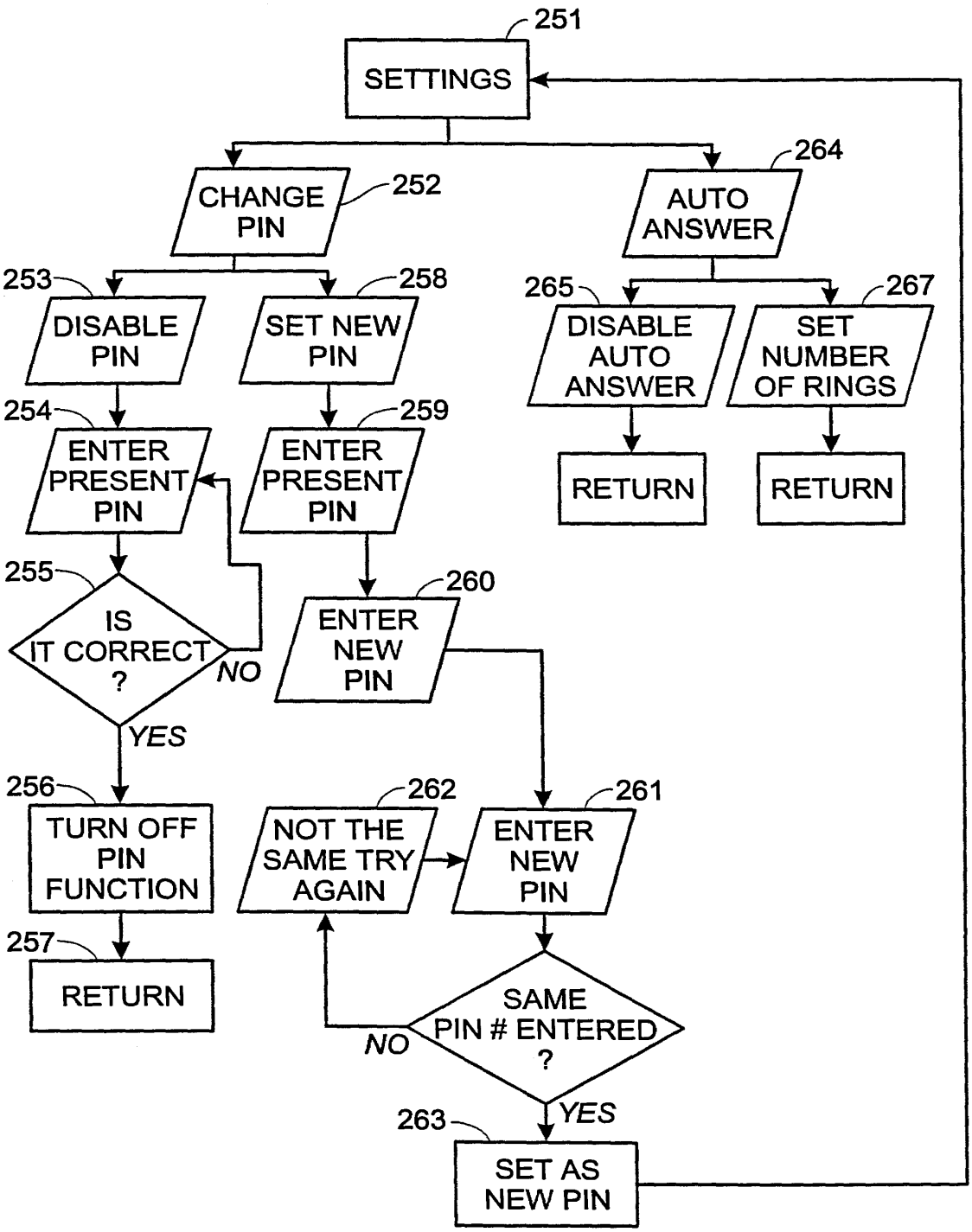

251
SETTINGS
CHANGE PIN
252
AUTO ANSWER
264
253
DISABLE PIN
258
SET NEW PIN
265
DISABLE AUTO ANSWER
267
SET NUMBER OF RINGS
254
ENTER PRESENT PIN
259
ENTER PRESENT PIN
RETURN
RETURN
255
IS IT CORRECT ?
NO
YES
260
ENTER NEW PIN
256
TURN OFF PIN FUNCTION
262
NOT THE SAME TRY AGAIN
261
ENTER NEW PIN
257
RETURN
SAME PIN # ENTERED ?
NO
YES
263
SET AS NEW PIN

Fig. 11

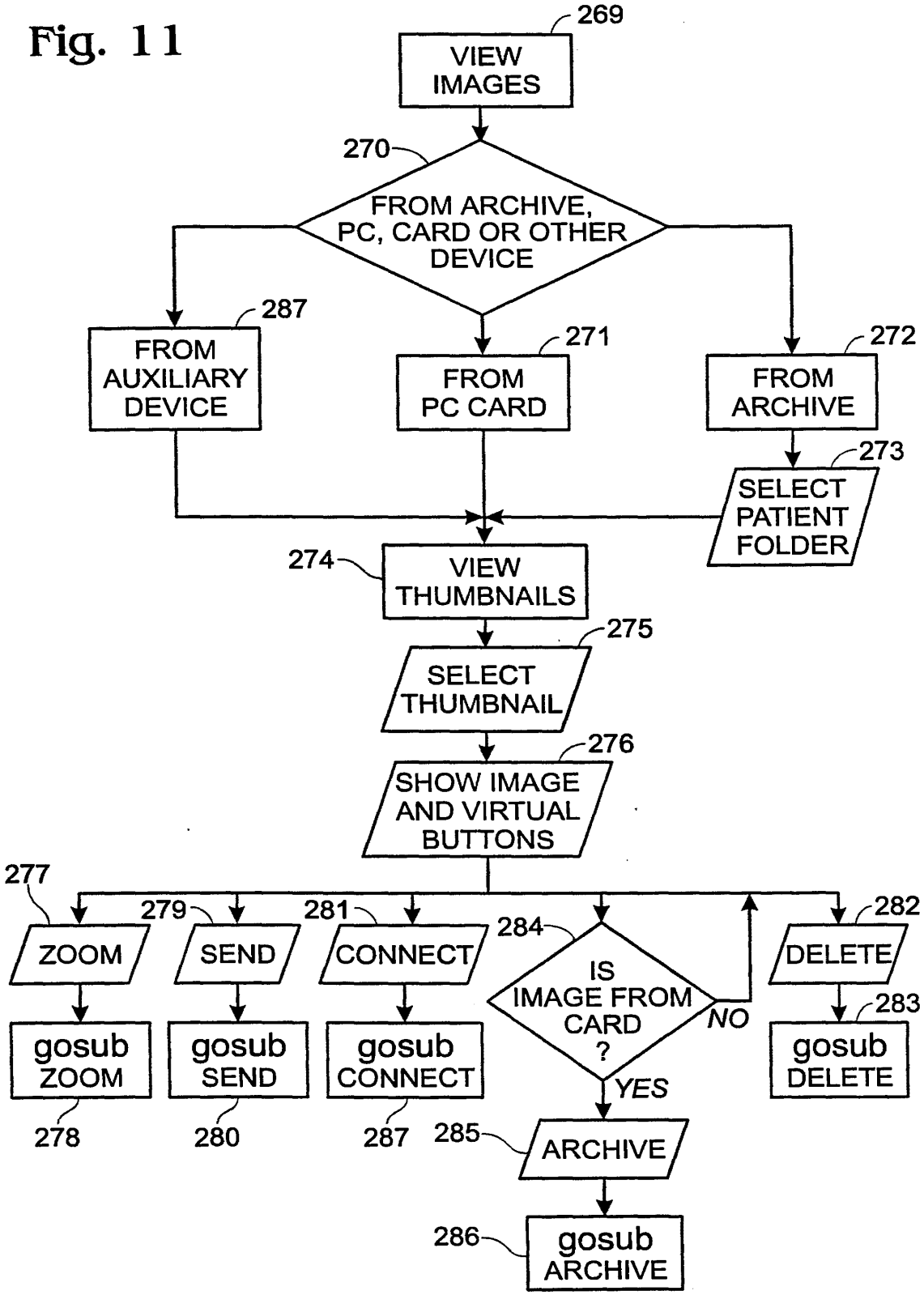

269
VIEW IMAGES
270
FROM ARCHIVE, PC, CARD OR OTHER DEVICE
287
FROM AUXILIARY DEVICE
271
FROM PC CARD
272
FROM ARCHIVE
273
SELECT PATIENT FOLDER
274
VIEW THUMBNAILS
275
SELECT THUMBNAIL
276
SHOW IMAGE AND VIRTUAL BUTTONS
277
ZOOM
279
SEND
281
CONNECT
284
IS IMAGE FROM CARD ?
NO
YES
282
DELETE
283
gosub DELETE
gosub ZOOM
gosub SEND
gosub CONNECT
278
280
287
285
ARCHIVE
286
gosub ARCHIVE

Fig. 12

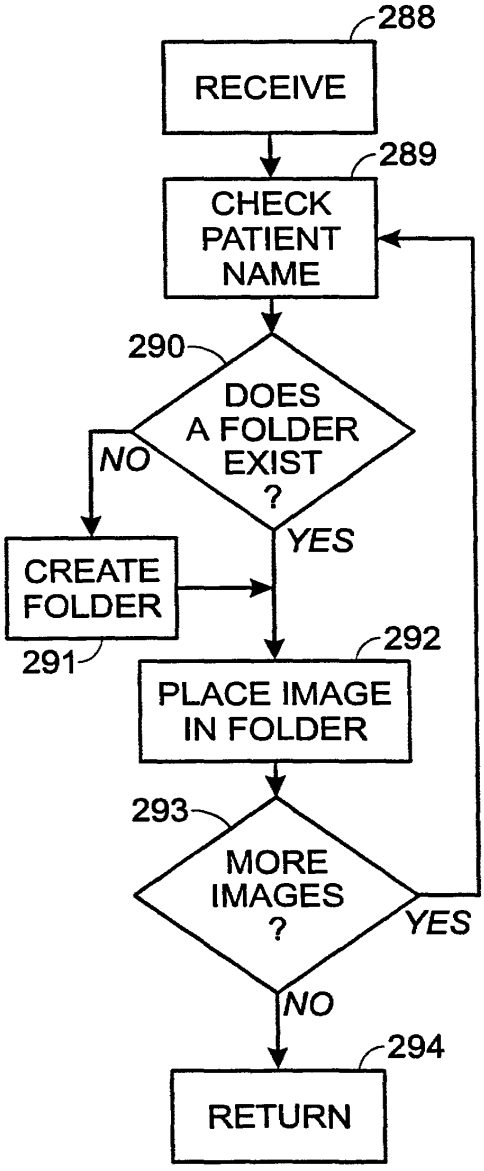

288
RECEIVE
289
CHECK PATIENT NAME
290
DOES A FOLDER EXIST ?
NO
YES
CREATE FOLDER
291
292
PLACE IMAGE IN FOLDER
293
MORE IMAGES ?
YES
NO
294
RETURN

Fig. 16

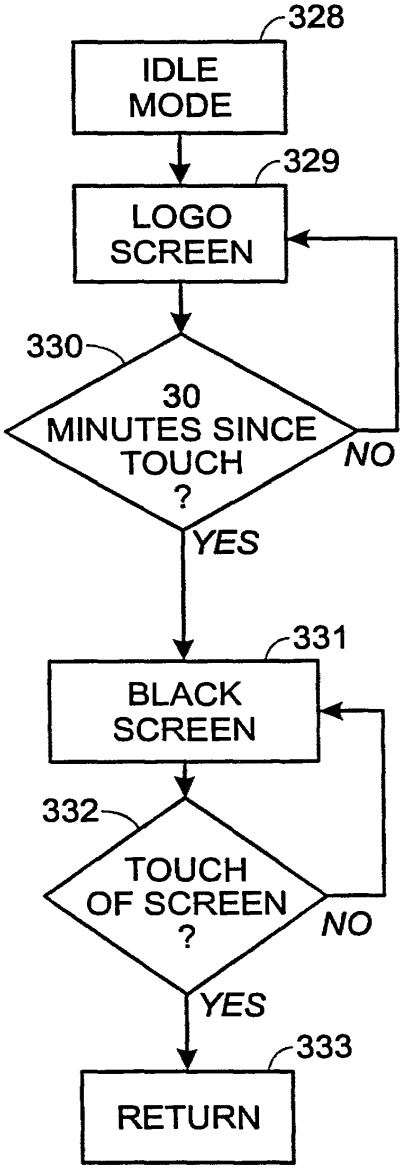
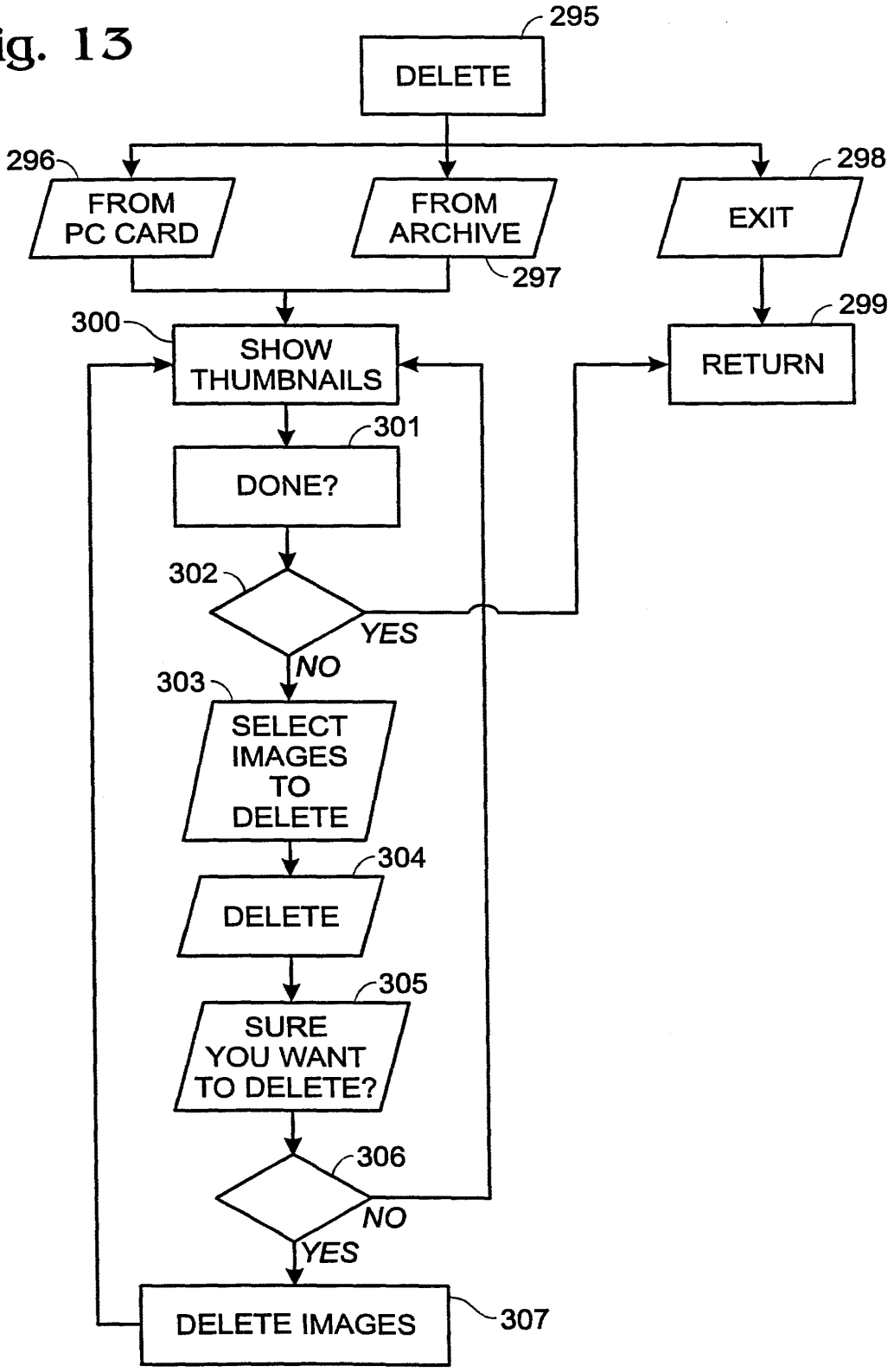

328
IDLE MODE
329
LOGO SCREEN
330
30 MINUTES SINCE TOUCH ?
NO
YES
331
BLACK SCREEN
332
TOUCH OF SCREEN ?
NO
YES
333
RETURN

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

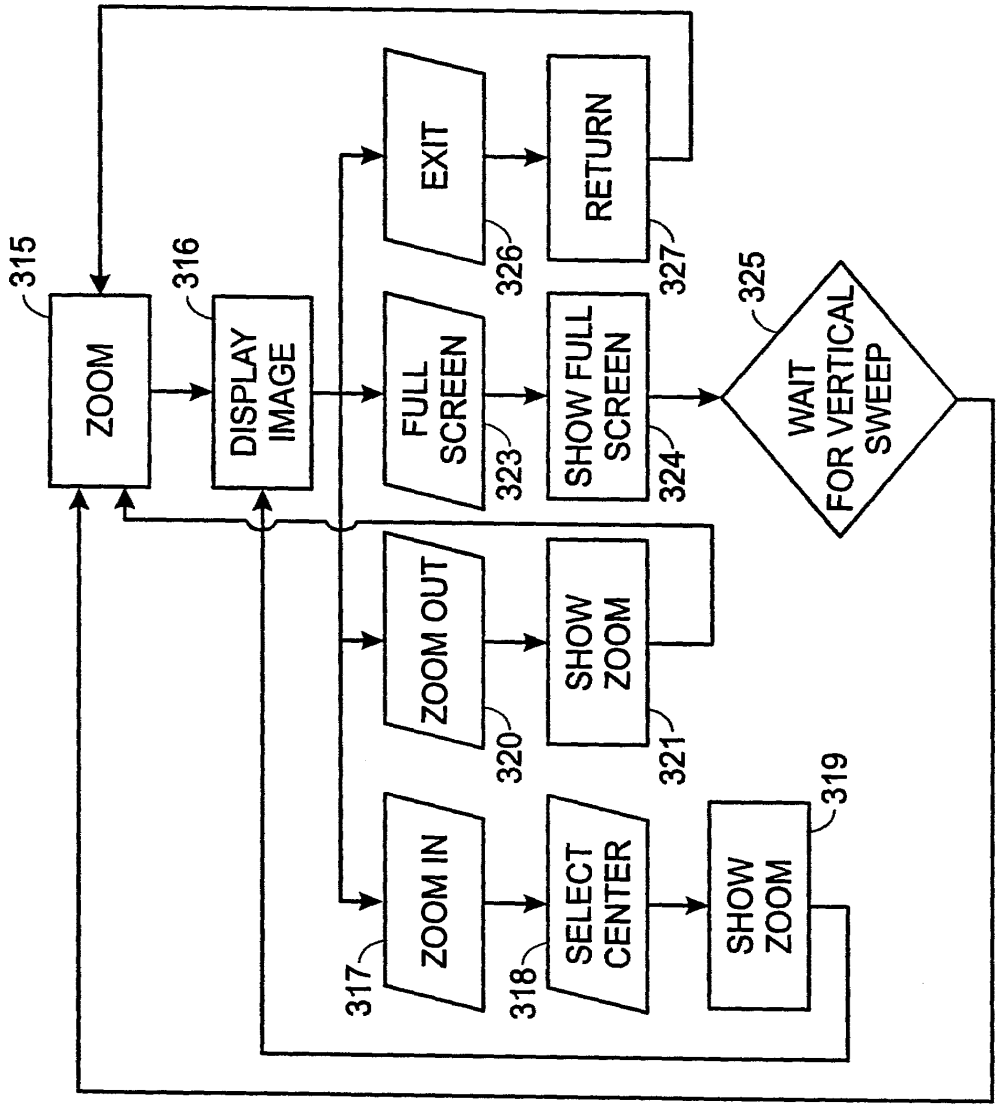

ZOOM
315
DISPLAY IMAGE
316
FULL SCREEN
323
EXIT
326
SHOW FULL SCREEN
324
RETURN
327
WAIT FOR VERTICAL SWEEP
325
ZOOM OUT
320
SHOW ZOOM
321
ZOOM IN
317
SELECT CENTER
318
SHOW ZOOM
319

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	Date of mailing of the international search report
04 OCTOBER 1998	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) 308-6603

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

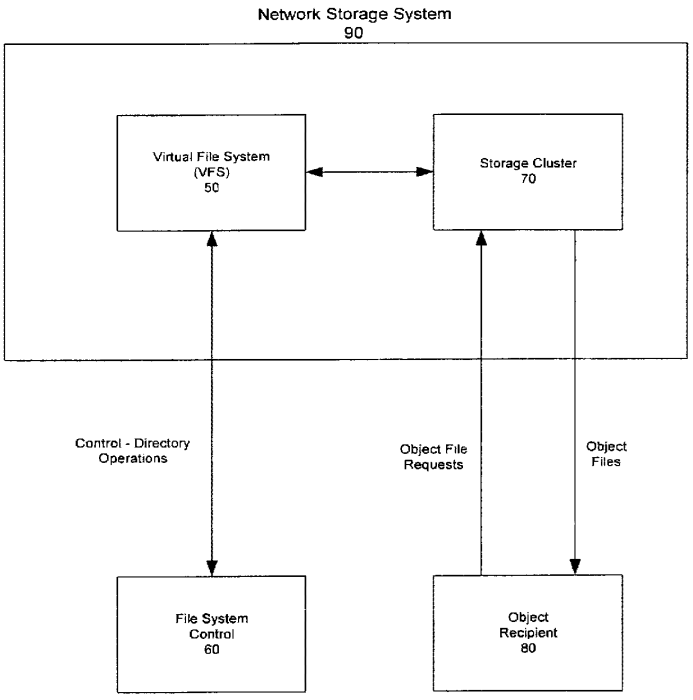
(75) Inventors/Applicants *(for US only)*: **COATES, Joshua, L.** [US/US]; 70 Brookwood Road, Orinda, CA 94563 (US). **JONES, F., Alan** [US/US]; 415 Pope Street, Menlo Park, CA 94025 (US). **RUSSEL, Georgina, L.** [US/US]; 899 Oak Street #4, San Francisco, CA 94117 (US). **GONZALEZ, Michael** [US/US]; 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 an error message is transmitted to the requester (blocks 1410 and 1415, Figure 14). If the request is validated, then the DDM extracts a file handler (*i.e.*, MD5 file handler) from the file table in the database (block 1420, Figure 14). The DDM deletes the file identification from the file table in the database (block 1450, Figure 14). In addition, the DDM constructs a delete SRL, and transmits the delete SRL to the storage cluster (block 1460, Figure 14). In response to the delete operation, the storage cluster extracts the reference count for the corresponding file. If the reference count is greater than 1, the storage cluster decrements the reference count by one (blocks 1430 and 1440, Figure 14). Alternatively, if the reference 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 the 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 and 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 a pool of resources. For the network storage system, the load balancing fabric 310 efficiently allocates requests among the "n" DOSMs. In one embodiment, when a DOSM transfers an object from the intelligent storage node to a destination, the object is cached in the data cache of the corresponding DOSM. Objects are deleted from the data cache in order to store 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 employed to identify data in high demand. Based on these decision mechanisms, data is cached in an attempt to meet the needs of the high demand. For example, an object may be in high demand when a movie studio offers, over its web site, a video preview of a newly released or upcoming film. For this example, the movie studio uses the network storage system to deliver the media rich object, "New Film Preview." The "New Film Preview" may be 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

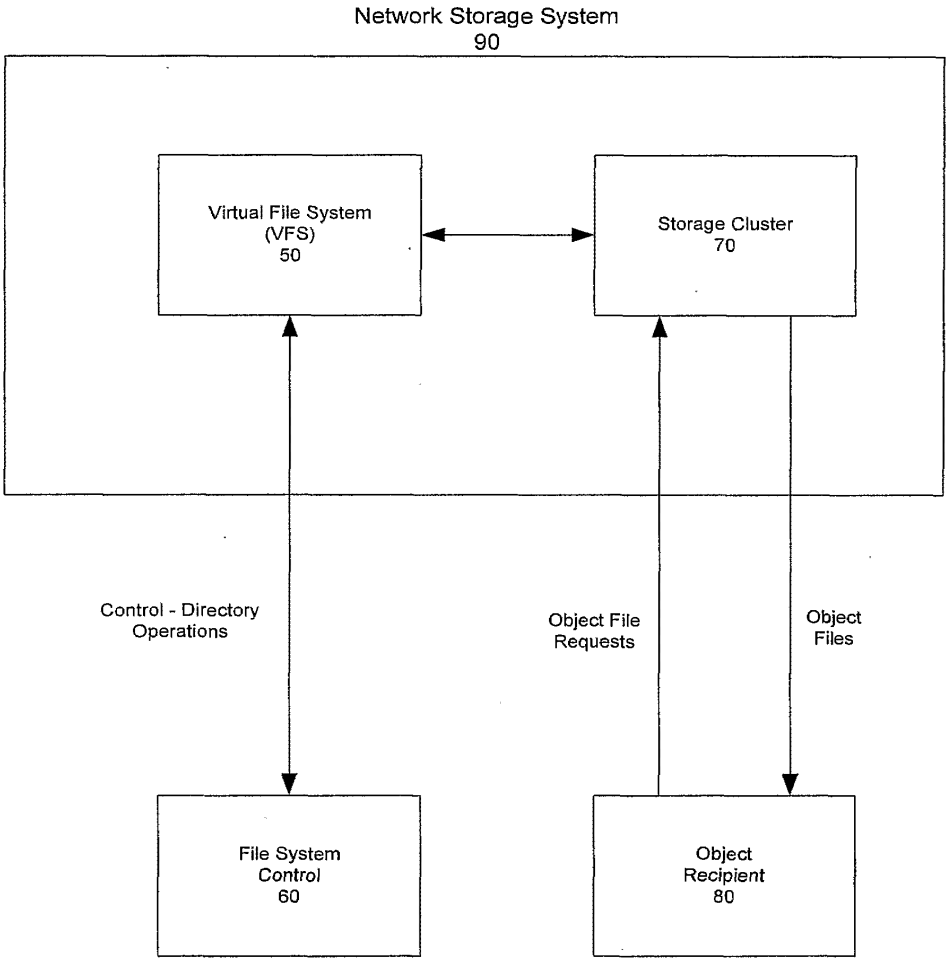

Network Storage System
90
Virtual File System
(VFS)
50
Storage Cluster
70
Control - Directory
Operations
Object File
Requests
Object
Files
File System
Control
60
Object
Recipient
80

Figure 1

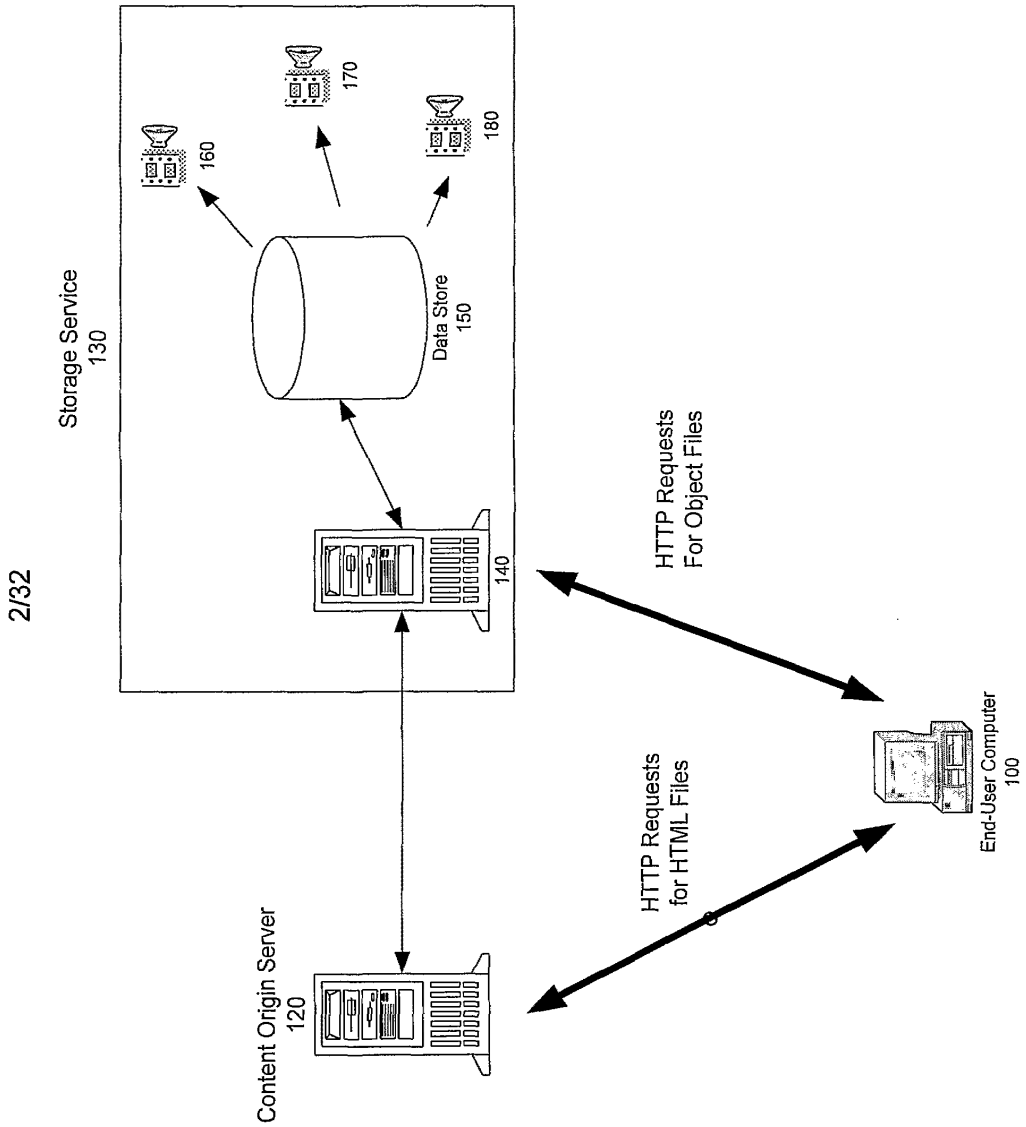

Storage Service
130
160
170
180
Data Store
150
140
HTTP Requests
For Object Files
HTTP Requests
for HTML Files
End-User Computer
100
Content Origin Server
120

Figure 2

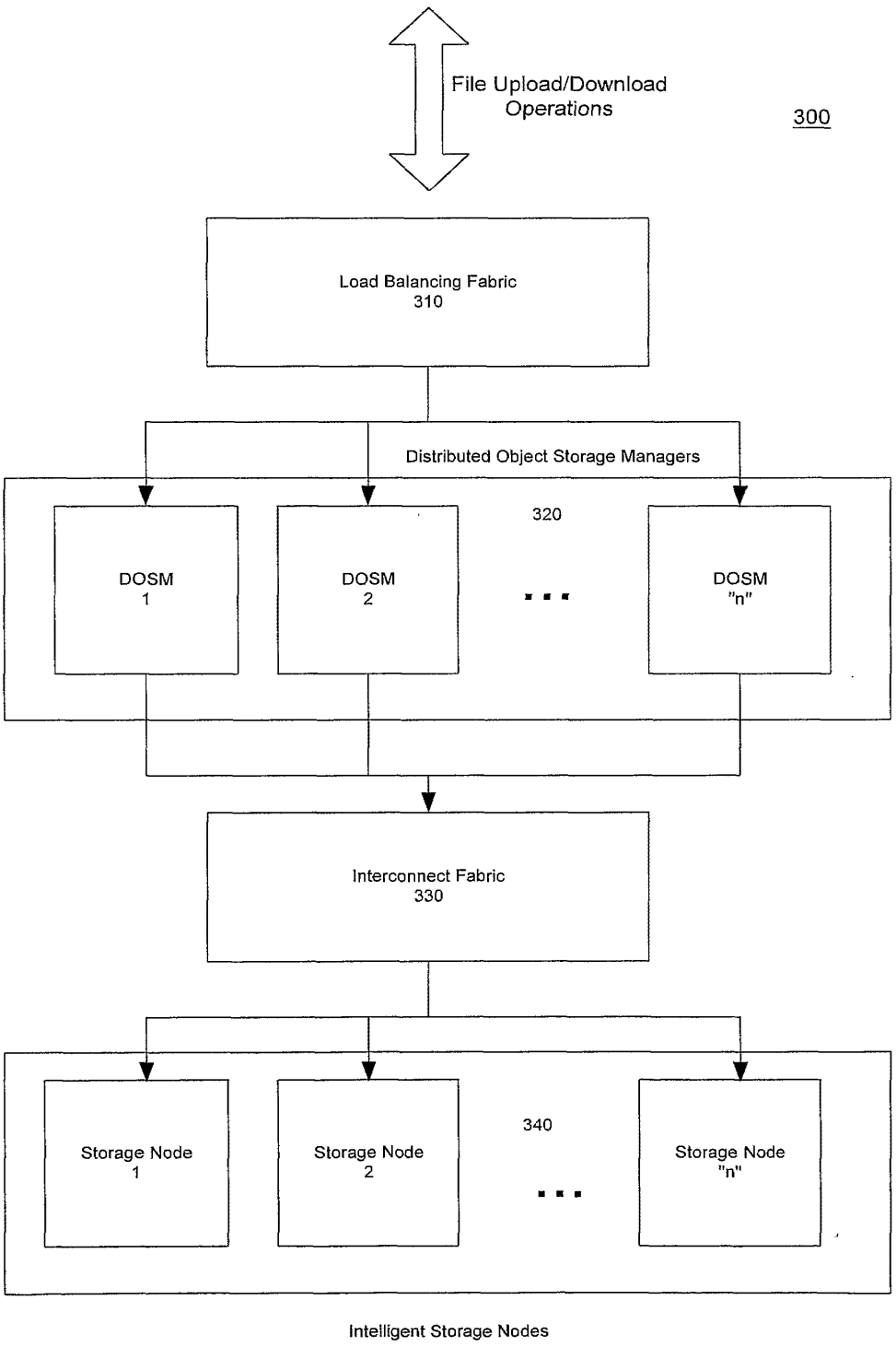

File Upload/Download Operations
300
Load Balancing Fabric 310
Distributed Object Storage Managers
320
DOSM 1
DOSM 2
DOSM "n"
Interconnect Fabric 330
340
Storage Node 1
Storage Node 2
Storage Node "n"
Intelligent Storage Nodes

Figure 3

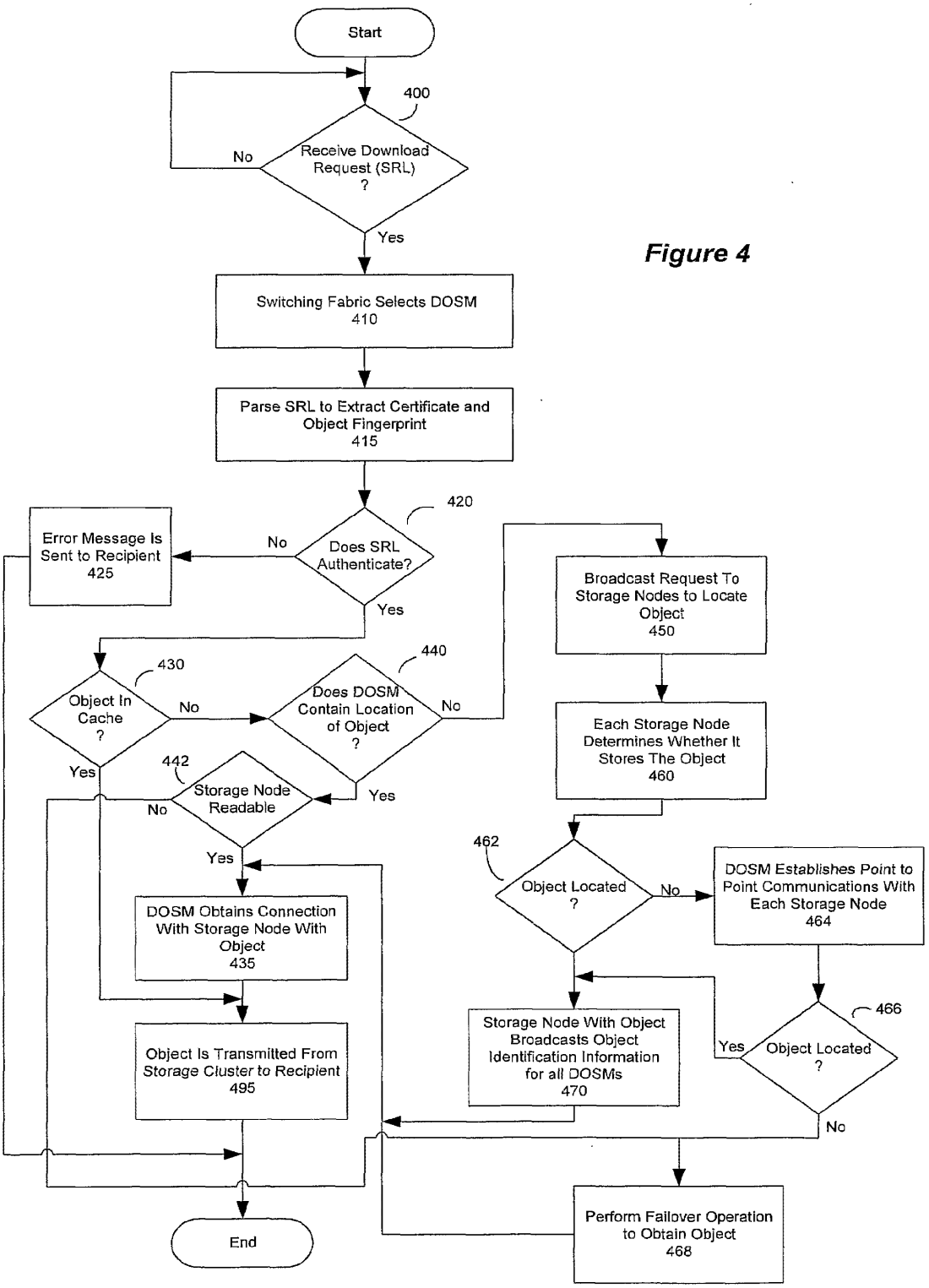

Start
400
Receive Download Request (SRL) ?
No
Yes
Switching Fabric Selects DOSM 410
Parse SRL to Extract Certificate and Object Fingerprint 415
420
Does SRL Authenticate?
No
Error Message Is Sent to Recipient 425
Yes
430
Object In Cache ?
No
440
Does DOSM Contain Location of Object ?
No
Yes
442
Storage Node Readable
No
Yes
Yes
DOSM Obtains Connection With Storage Node With Object 435
Object Is Transmitted From Storage Cluster to Recipient 495
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
466
Yes
Object Located ?
No
Storage Node With Object Broadcasts Object Identification Information for all DOSMs 470
Perform Failover Operation to Obtain Object 468
End

Figure 4

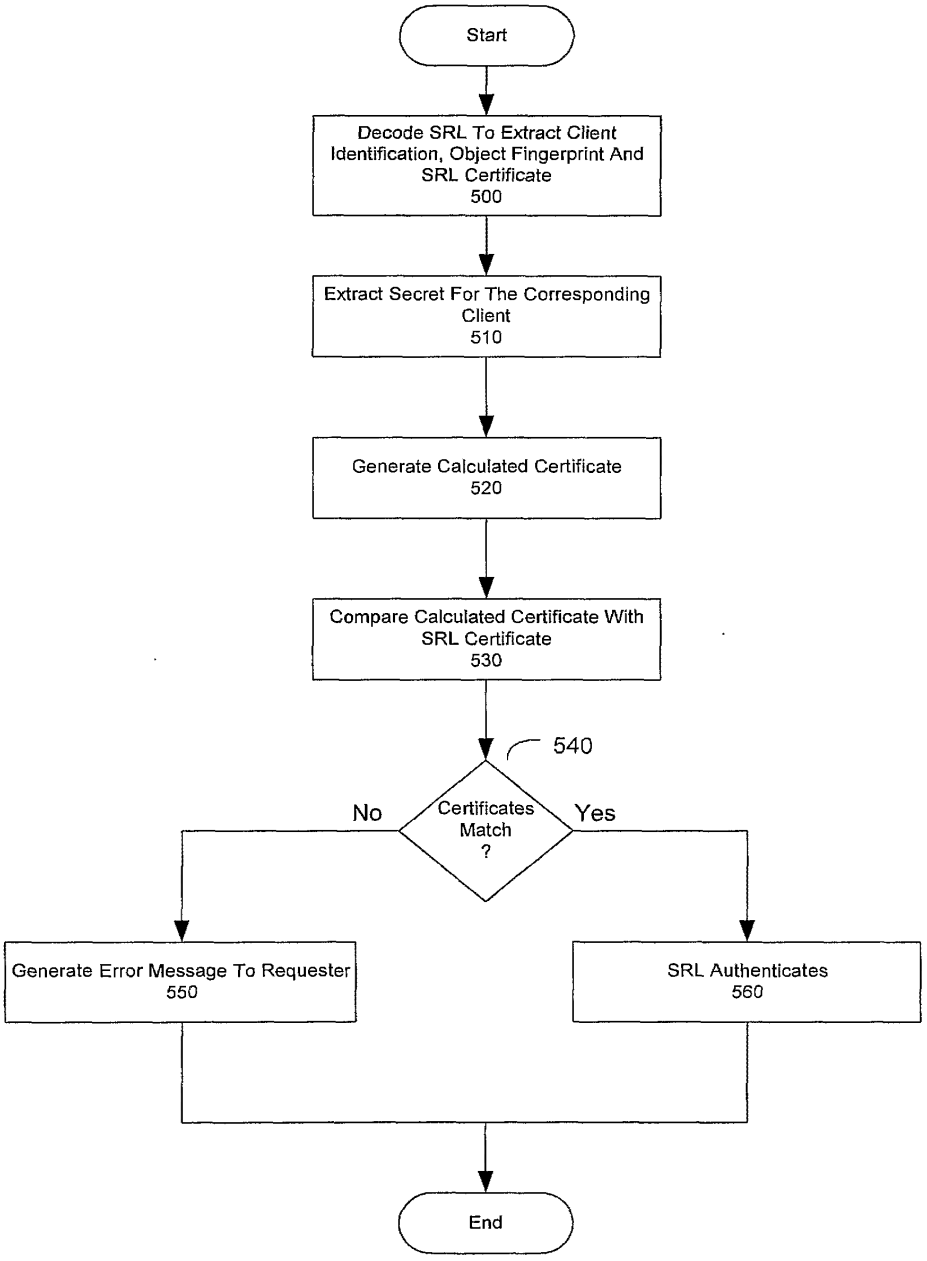

Start
Decode SRL To Extract Client Identification, Object Fingerprint And SRL Certificate
500
Extract Secret For The Corresponding Client
510
Generate Calculated Certificate
520
Compare Calculated Certificate With SRL Certificate
530
540
Certificates Match ?
No
Yes
Generate Error Message To Requester
550
SRL Authenticates
560
End

Figure 5

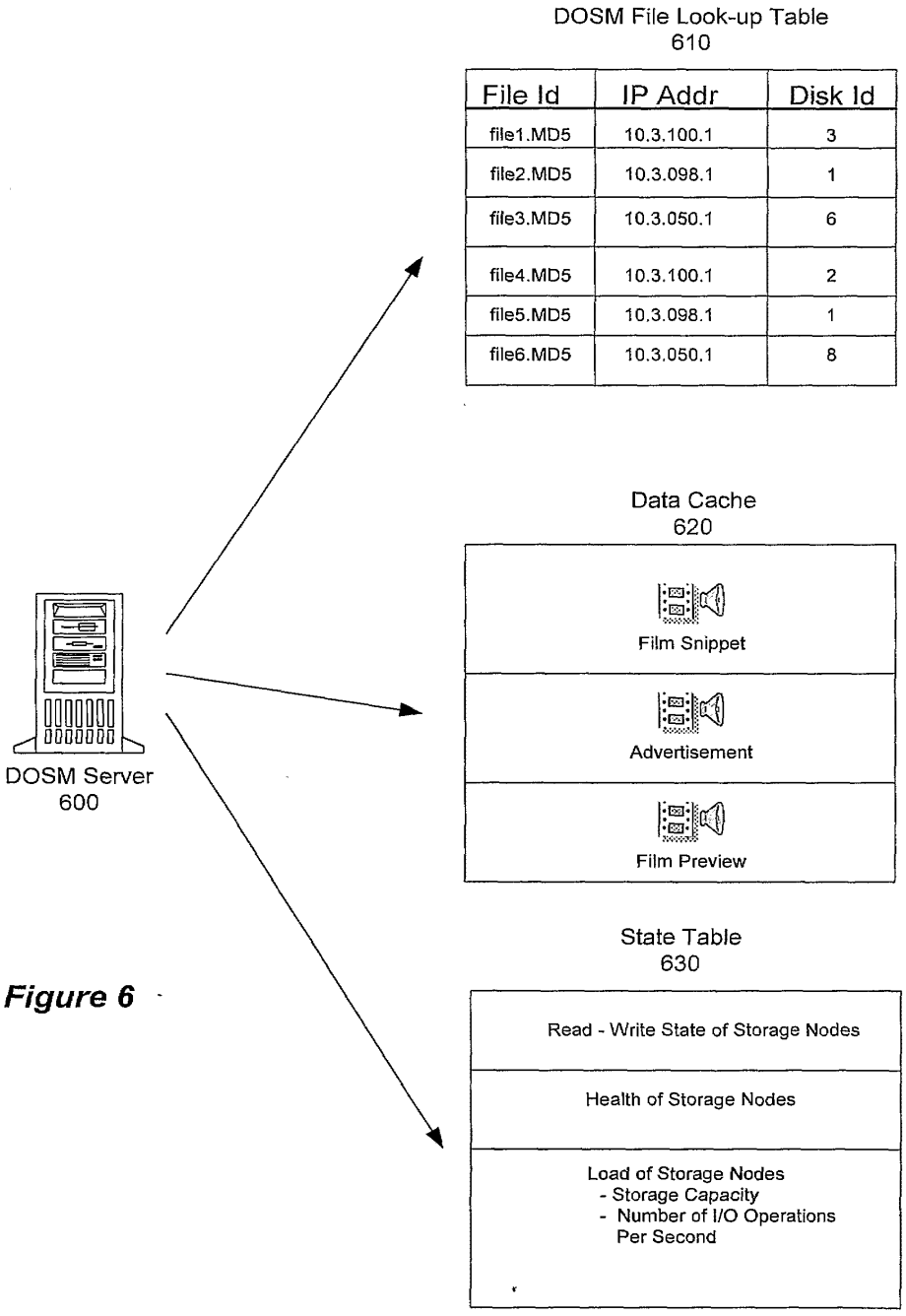

DOSM File Look-up Table
610
File Id
IP Addr
Disk Id
file1.MD5
10.3.100.1
3
file2.MD5
10.3.098.1
1
file3.MD5
10.3.050.1
6
file4.MD5
10.3.100.1
2
file5.MD5
10.3.098.1
1
file6.MD5
10.3.050.1
8
Data Cache
620
Film Snippet
Advertisement
Film Preview
DOSM Server
600
State Table
630
Read - Write State of Storage Nodes
Health of Storage Nodes
Load of Storage Nodes
- Storage Capacity
- Number of I/O Operations Per Second

Figure 6

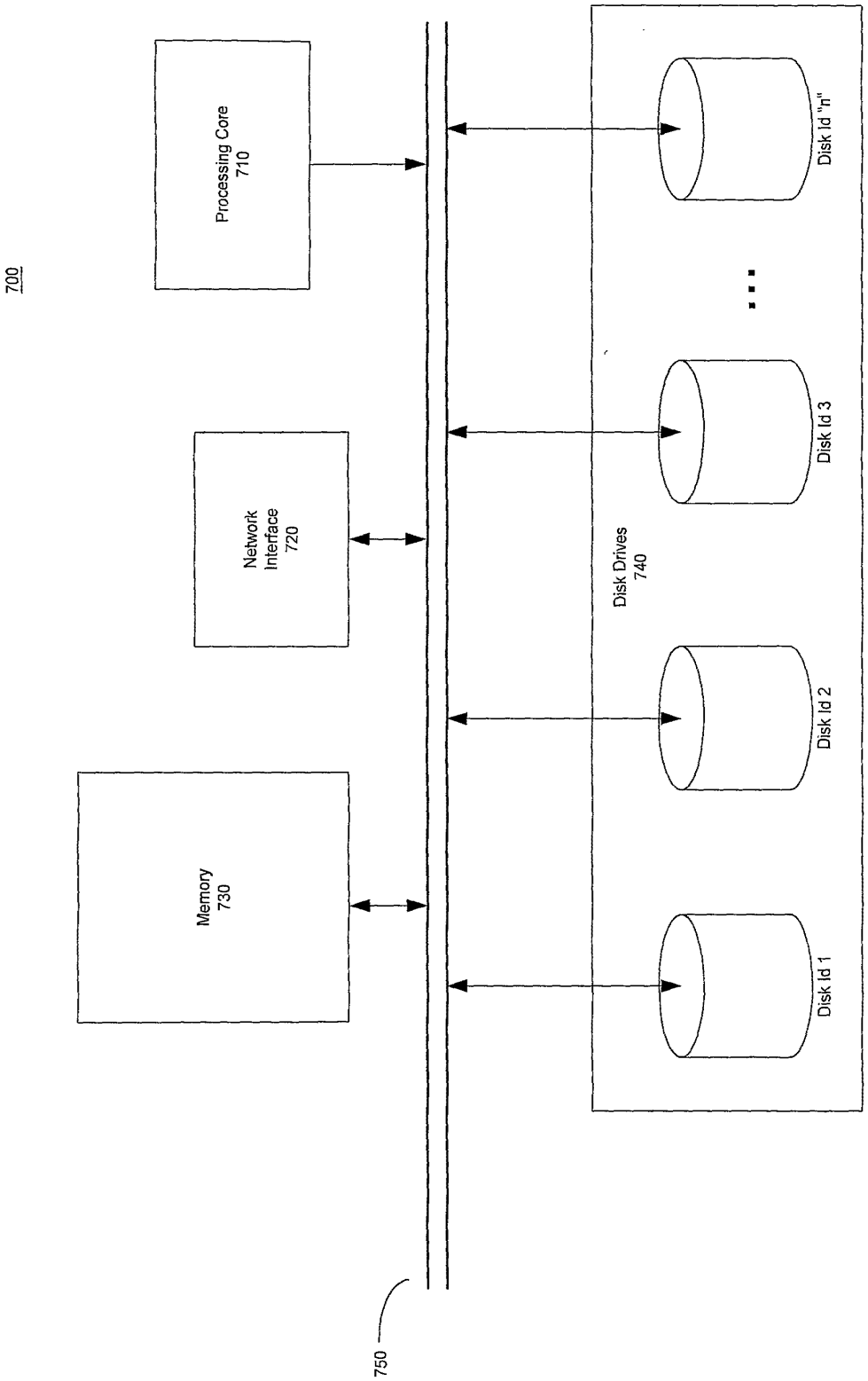

700
Processing Core
710
Network
Interface
720
Memory
730
750
Disk Drives
740
Disk Id 1
Disk Id 2
Disk Id 3
Disk Id "n"

Figure 7

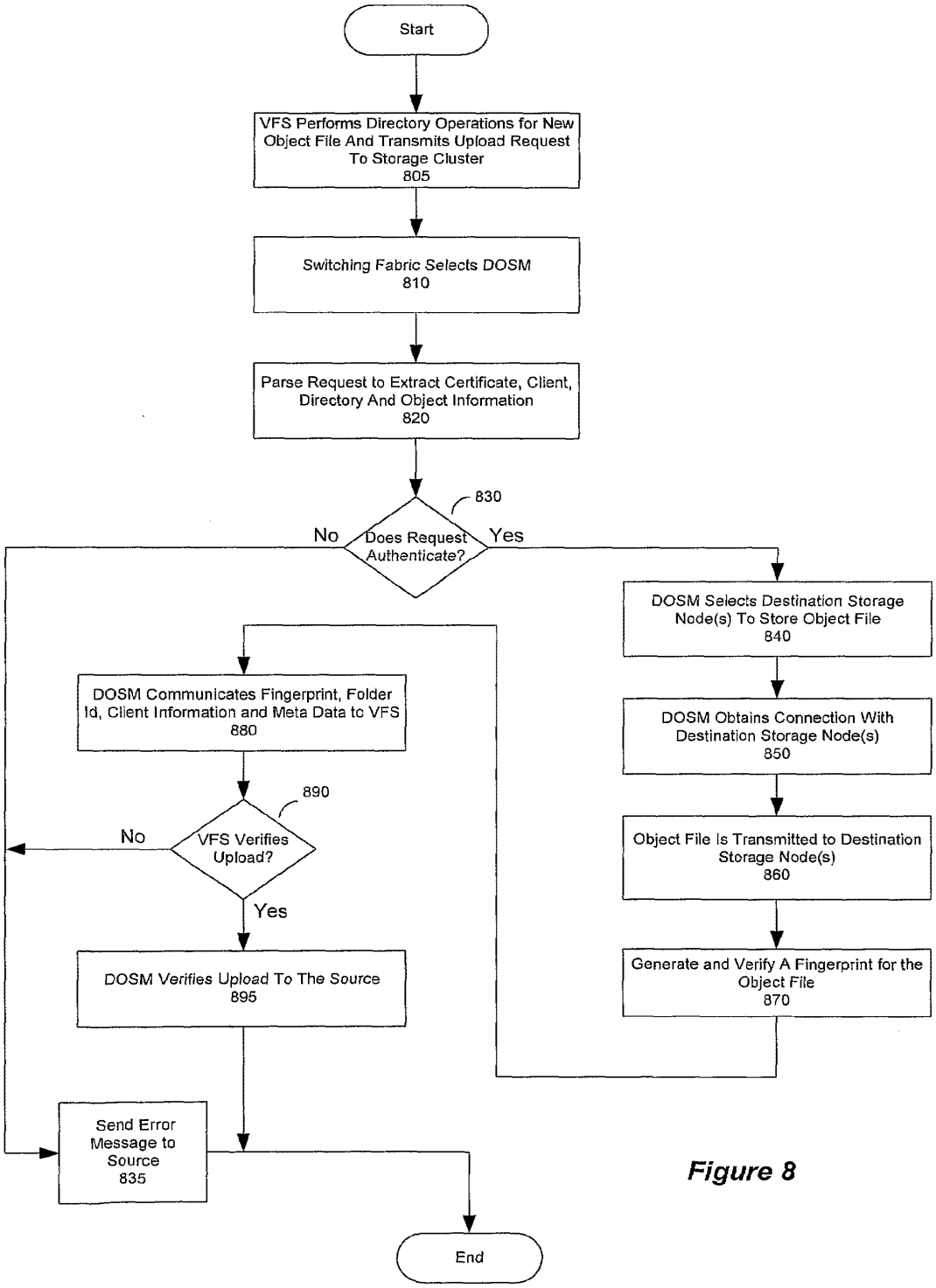

Start
VFS Performs Directory Operations for New Object File And Transmits Upload Request To Storage Cluster
805
Switching Fabric Selects DOSM
810
Parse Request to Extract Certificate, Client, Directory And Object Information
820
830
Does Request Authenticate?
No
Yes
DOSM Selects Destination Storage Node(s) 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

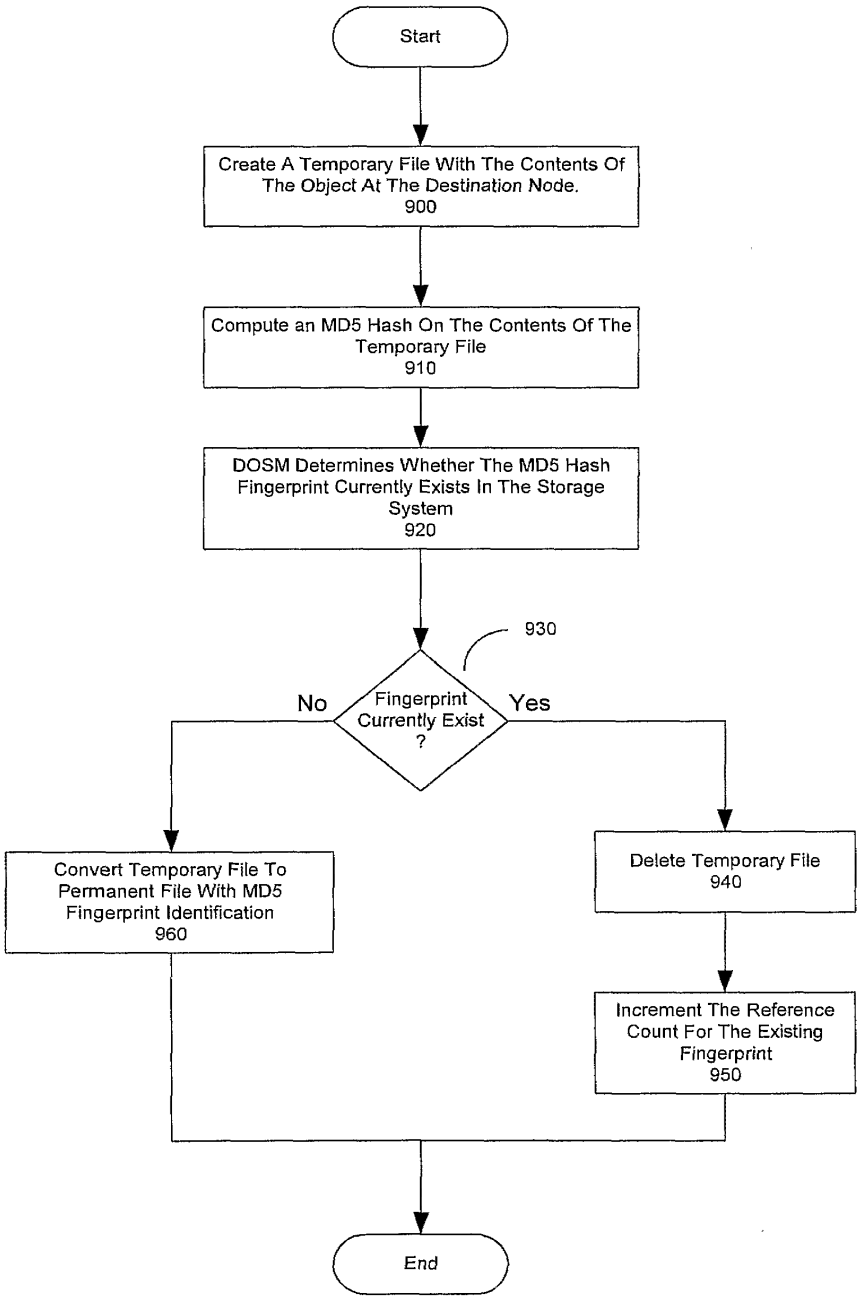
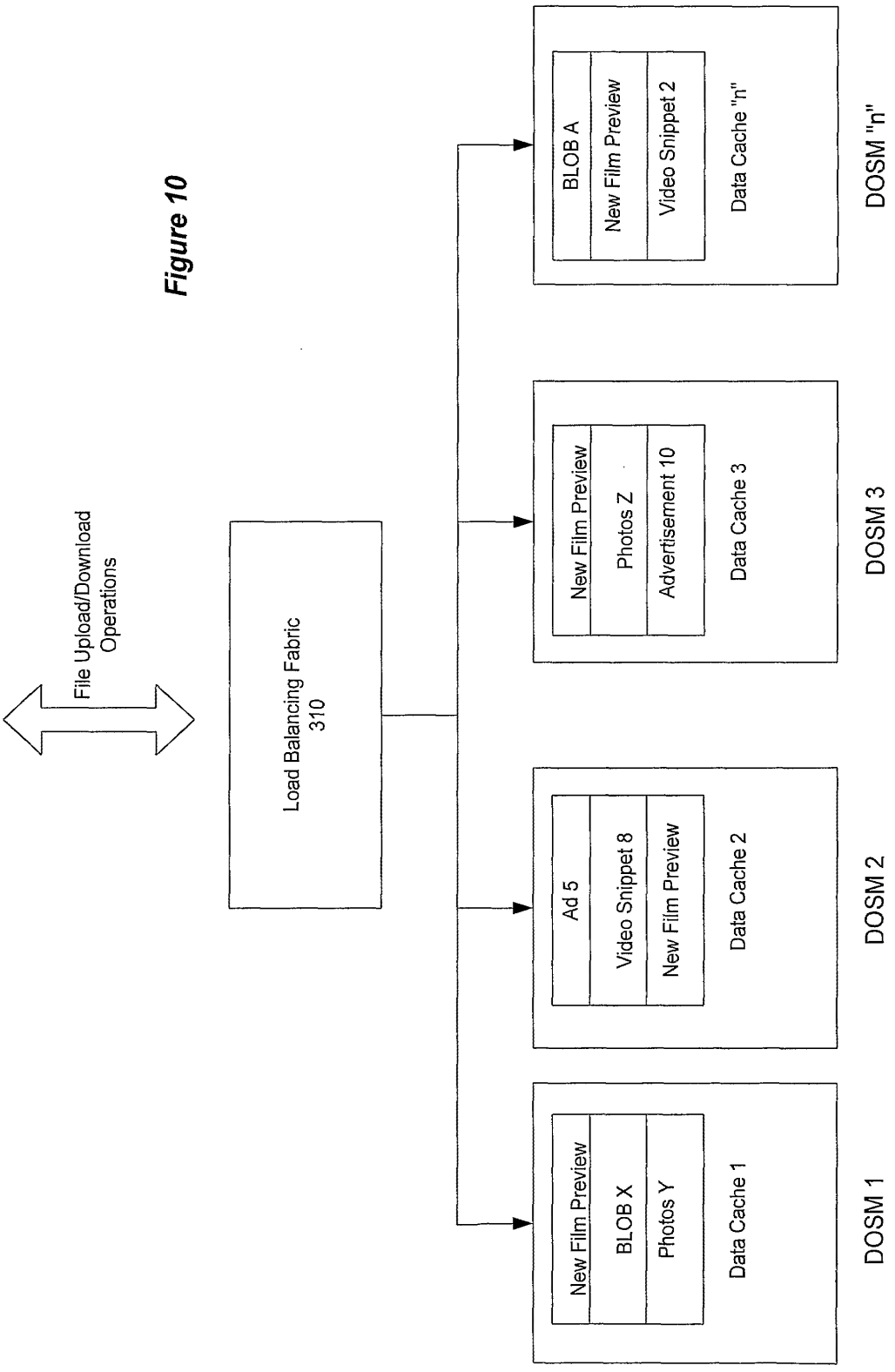

Start
Create A Temporary File With The Contents Of The Object At The Destination Node.
900
Compute an MD5 Hash On The Contents Of The Temporary File
910
DOSM Determines Whether The MD5 Hash Fingerprint Currently Exists In The Storage System
920
930
Fingerprint Currently Exist ?
No
Yes
Convert Temporary 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

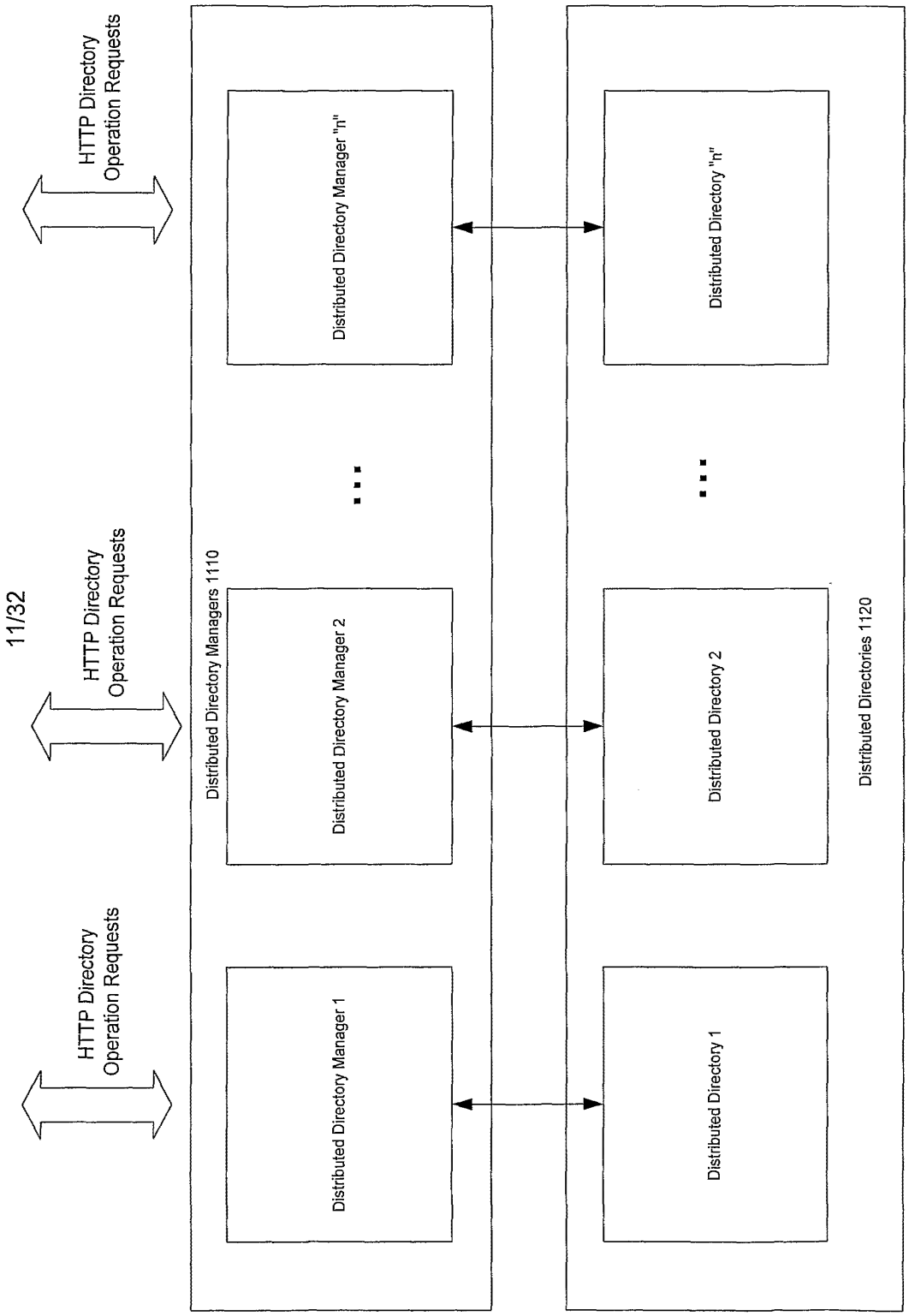

HTTP Directory Operation Requests
HTTP Directory Operation Requests
HTTP Directory Operation Requests
Distributed Directory Managers 1110
Distributed Directory Manager "n"
Distributed Directory Manager 2
Distributed Directory Manager 1
Distributed Directory "n"
Distributed Directory 2
Distributed Directory 1
Distributed Directories 1120
1100

Figure 11

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

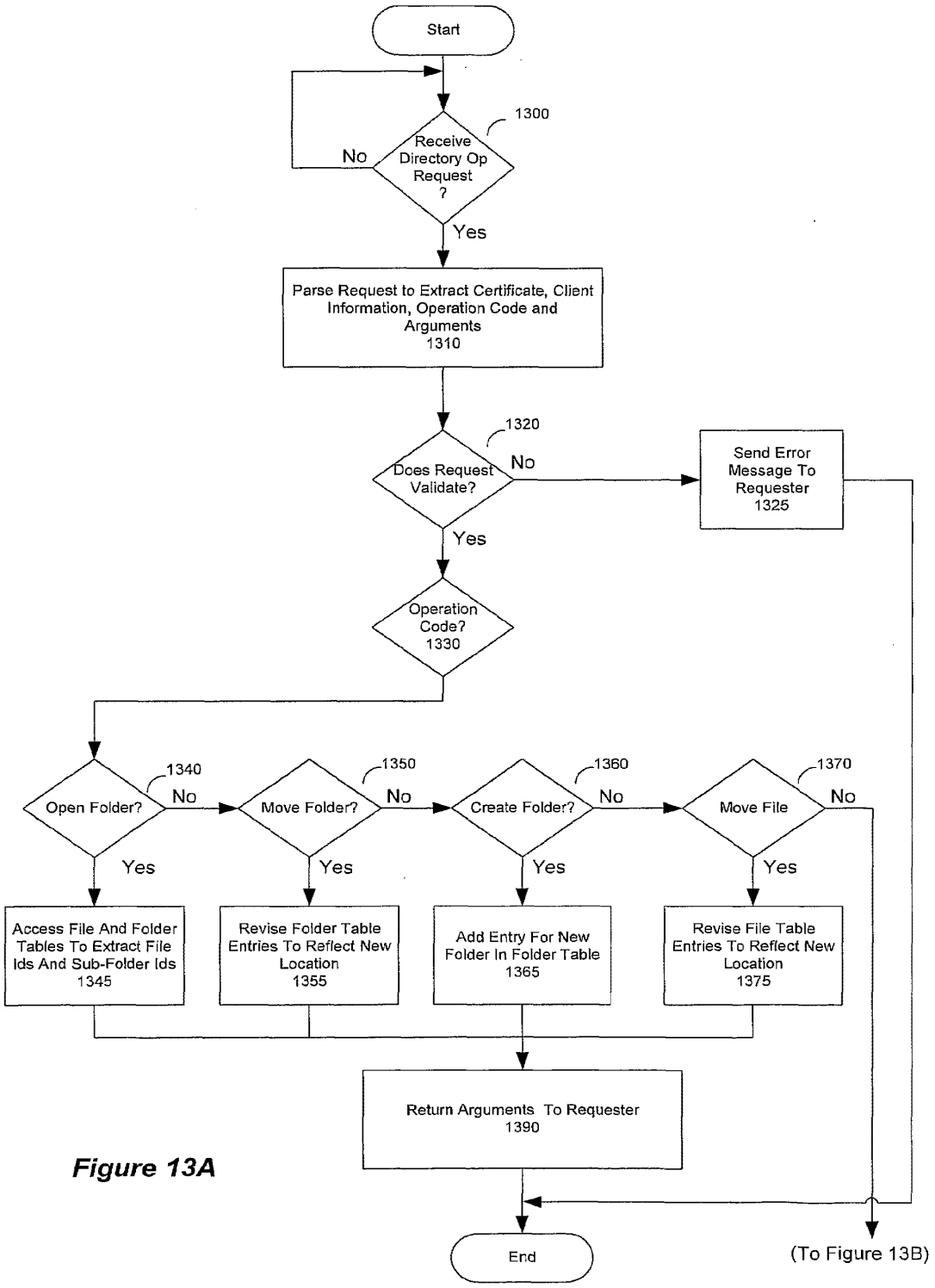

Start
1300
Receive Directory Op Request ?
No
Yes
Parse Request to Extract Certificate, Client Information, Operation Code and Arguments
1310
1320
Does Request Validate?
No
Send Error Message To Requester
1325
Yes
Operation Code?
1330
1340
Open Folder?
No
1350
Move Folder?
No
1360
Create Folder?
No
1370
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

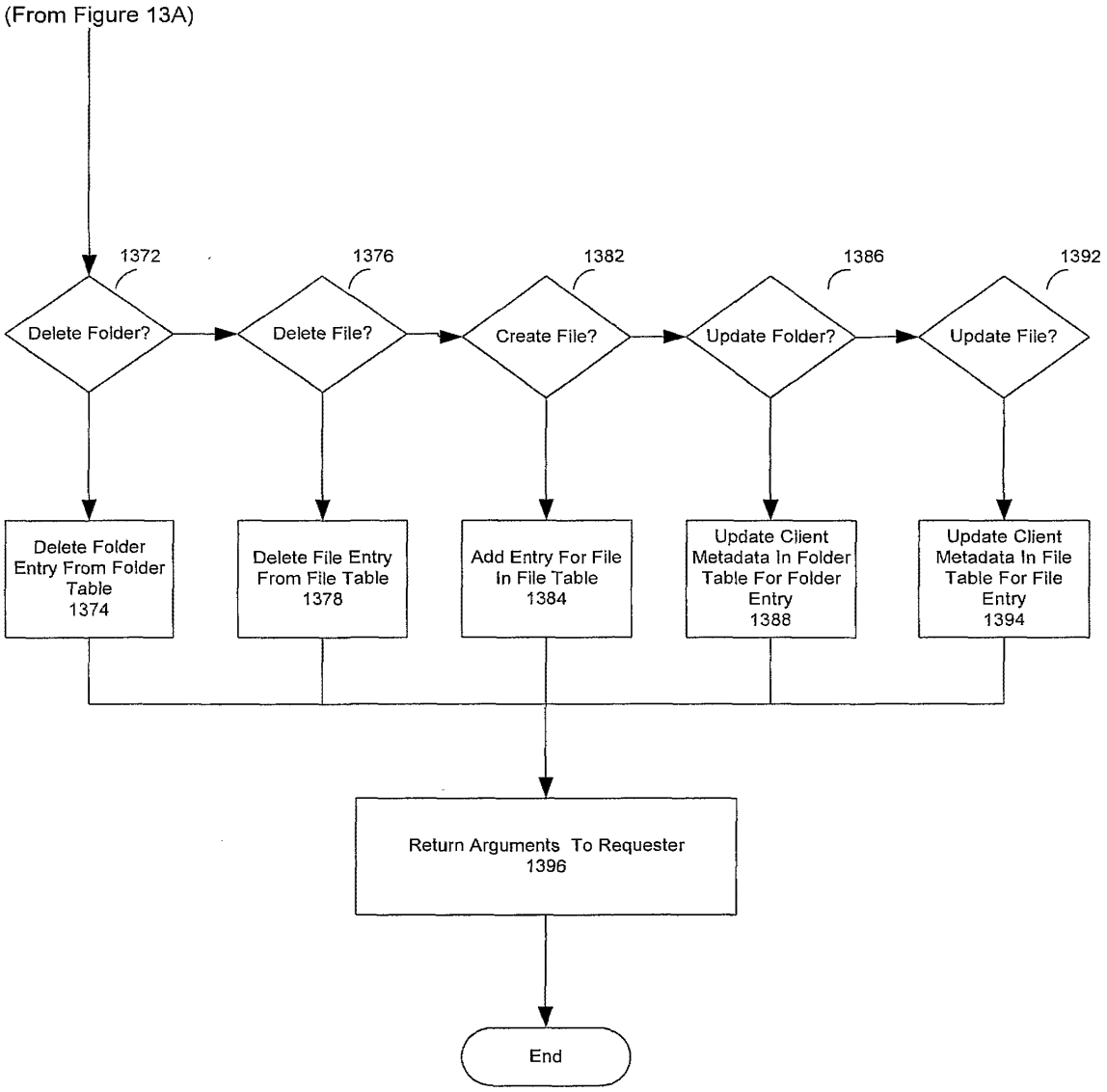

(From Figure 13A)
1372
Delete Folder?
1376
Delete File?
1382
Create File?
1386
Update Folder?
1392
Update File?
Delete Folder Entry From Folder Table 1374
Delete File Entry From File Table 1378
Add Entry For File In File Table 1384
Update Client Metadata In Folder Table For Folder Entry 1388
Update Client Metadata In File Table For File Entry 1394
Return Arguments To Requester 1396
End

Figure 13B

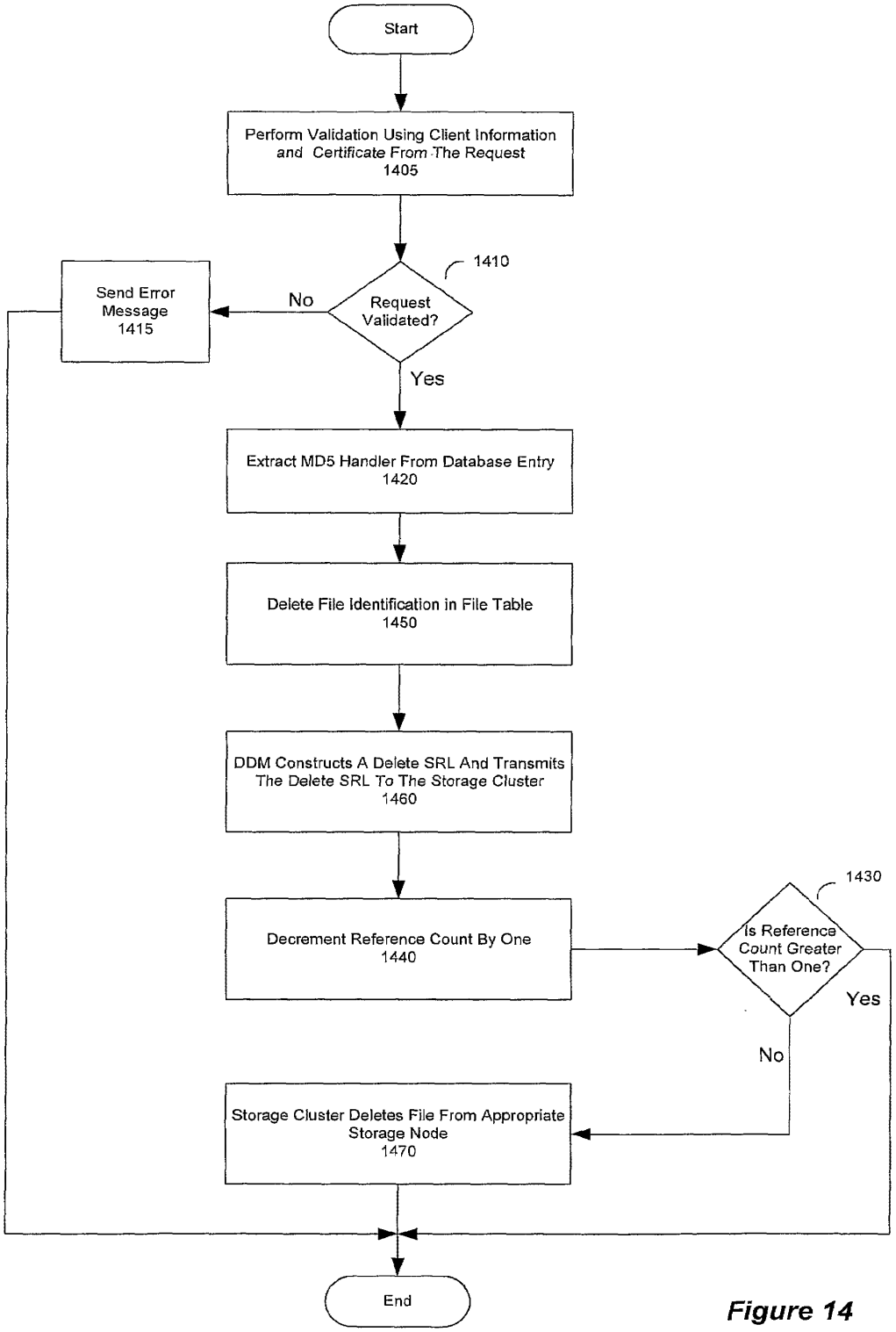

Start
Perform Validation Using Client Information and Certificate From The Request
1405
1410
Request Validated?
No
Send Error Message
1415
Yes
Extract MD5 Handler From Database Entry
1420
Delete File Identification in File Table
1450
DDM Constructs A Delete SRL And Transmits The Delete SRL To The Storage 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

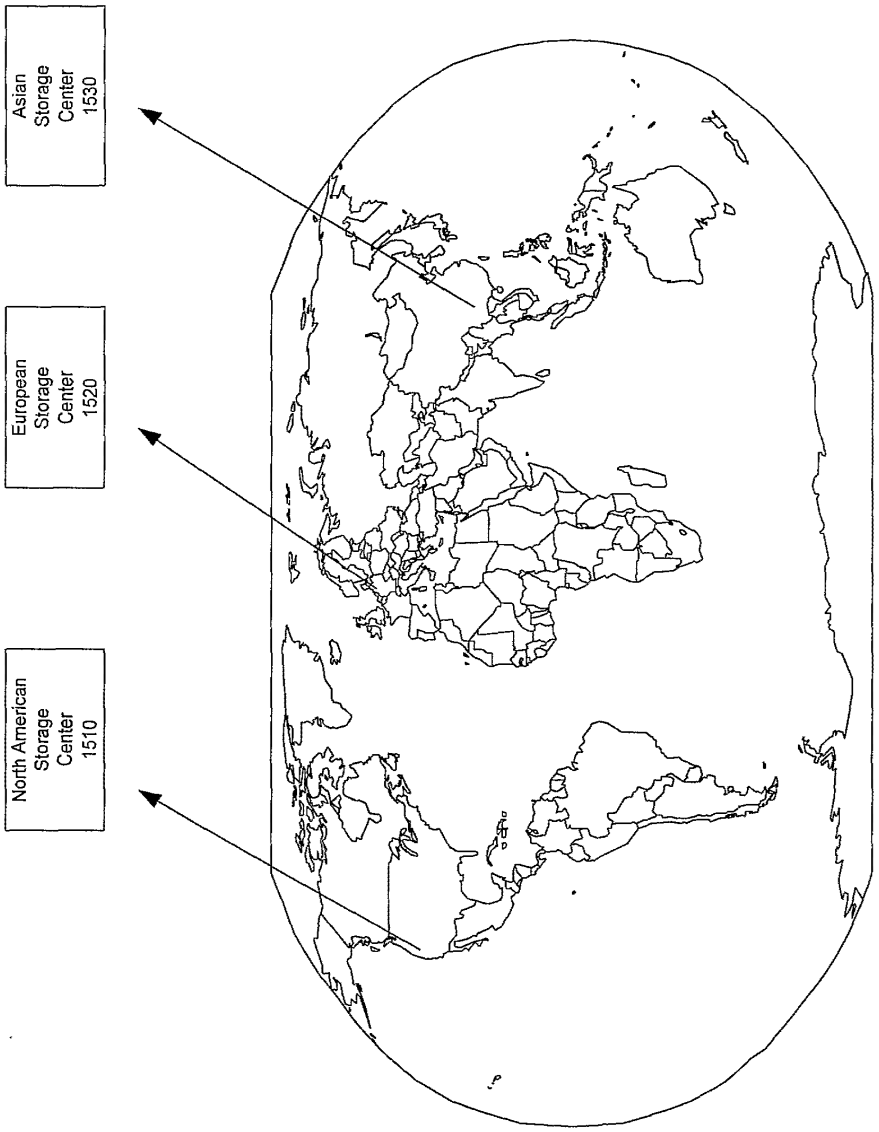

Asian Storage Center 1530
European Storage Center 1520
North American Storage Center 1510

Figure 15

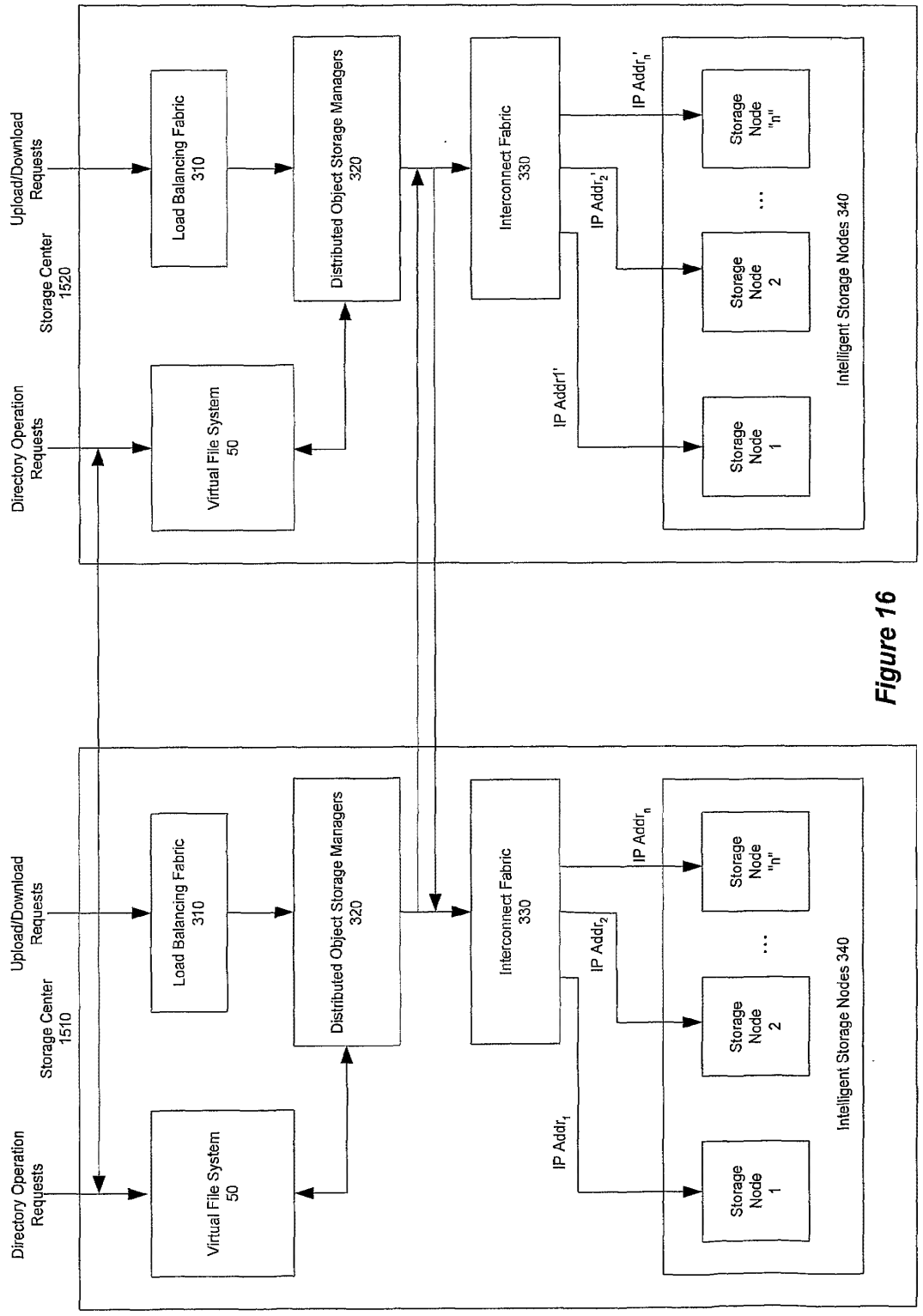

Storage Center 1520
Upload/Download Requests
Directory Operation Requests
Load Balancing Fabric 310
Virtual File System 50
Distributed Object Storage Managers 320
Interconnect Fabric 330
IP Addr1'
IP Addr2'
IP Addrn'
Storage Node 1
Storage Node 2
Storage Node "n"
Inteligent Storage Nodes 340
Storage 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"
Inteligent Storage Nodes 340

Figure 16

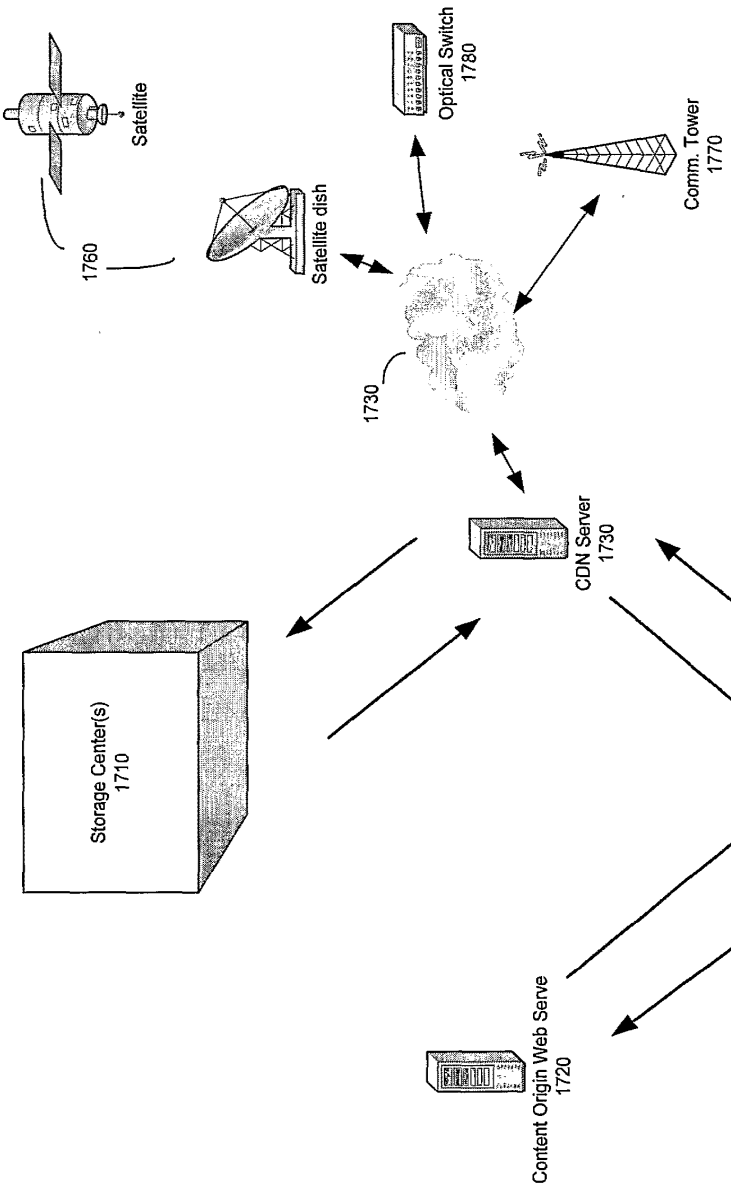

Satellite
1760
Satellite dish
Optical Switch
1780
Comm. Tower
1770
1730
CDN Server
1730
Storage Center(s)
1710
End-User
Computer
1740
Content Origin Web Serve
1720

Figure 17

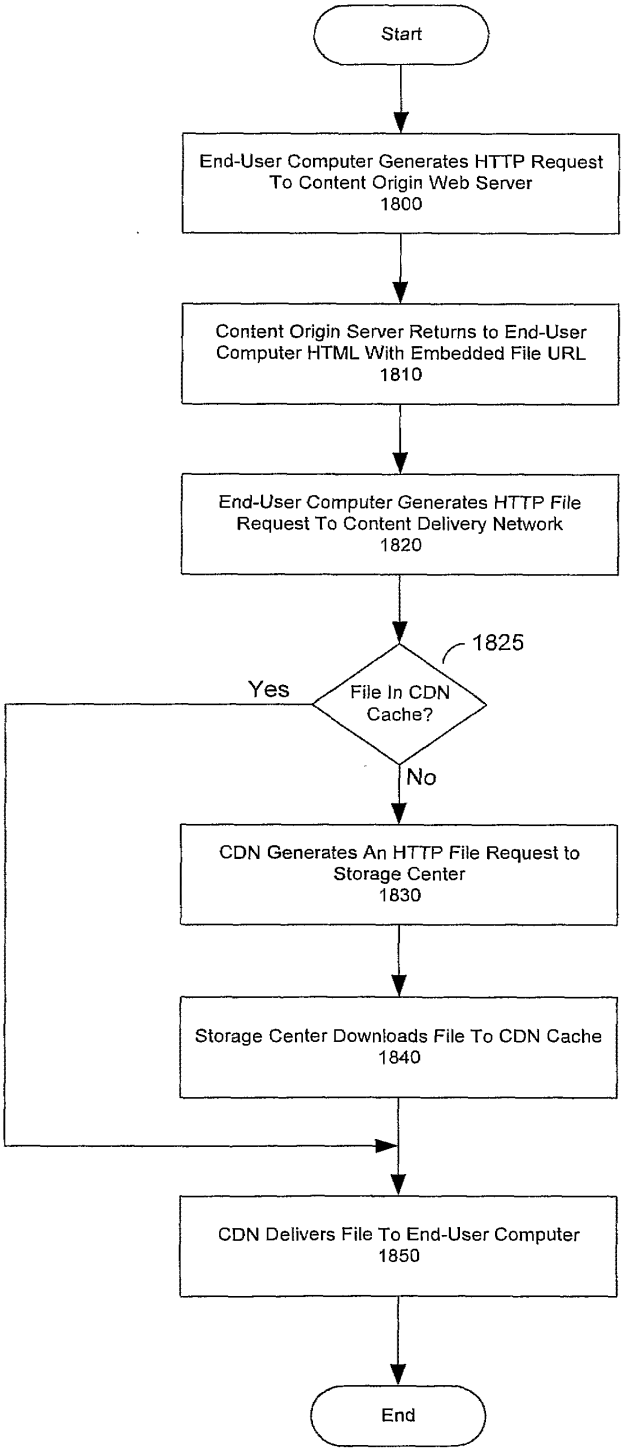

Start
End-User Computer Generates HTTP Request To Content Origin Web Server 1800
Content Origin Server Returns to End-User Computer HTML With Embedded File URL 1810
End-User Computer Generates HTTP File Request To Content Delivery Network 1820
1825
File In CDN Cache?
Yes
No
CDN Generates An HTTP File Request to Storage Center 1830
Storage Center Downloads File To CDN Cache 1840
CDN Delivers File To End-User Computer 1850
End

Figure 18

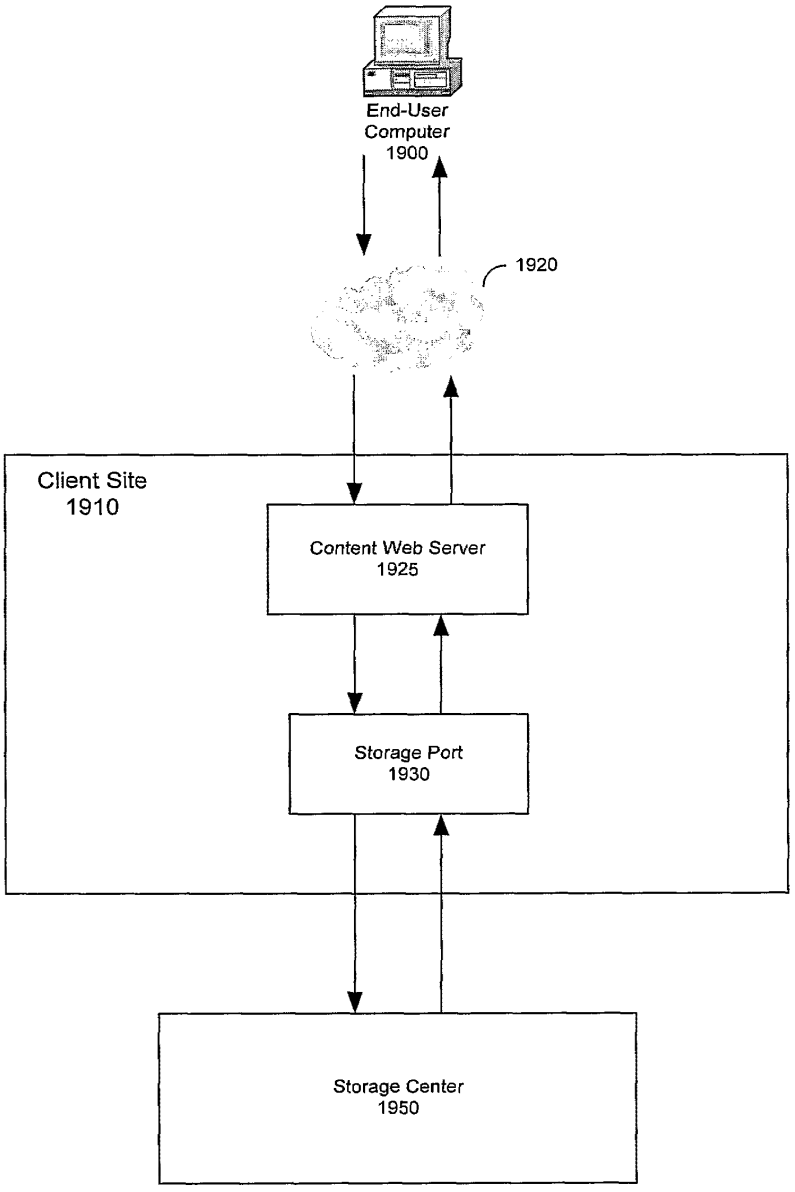

End-User
Computer
1900
1920
Client Site
1910
Content Web Server
1925
Storage Port
1930
Storage Center
1950

Figure 19

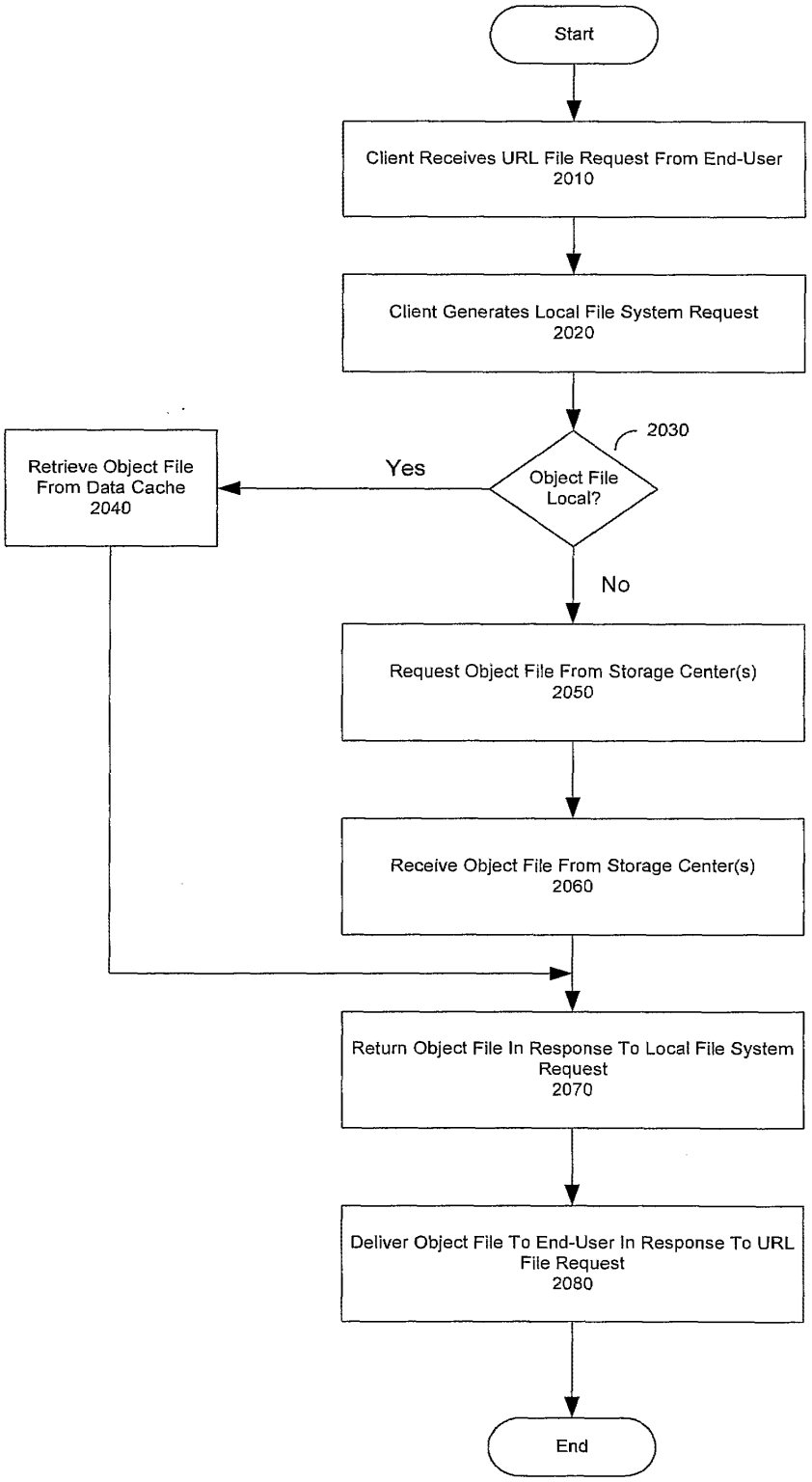

Start
Client Receives URL File Request From End-User
2010
Client Generates Local File System Request
2020
2030
Object File Local?
Yes
Retrieve Object File From Data Cache
2040
No
Request Object File From Storage Center(s)
2050
Receive Object File From Storage Center(s)
2060
Return Object File In Response To Local File System Request
2070
Deliver Object File To End-User In Response To URL File Request
2080
End

Figure 20

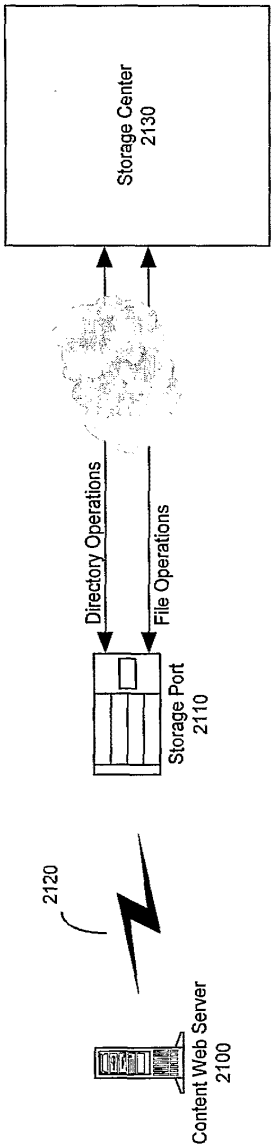


Figure 21a

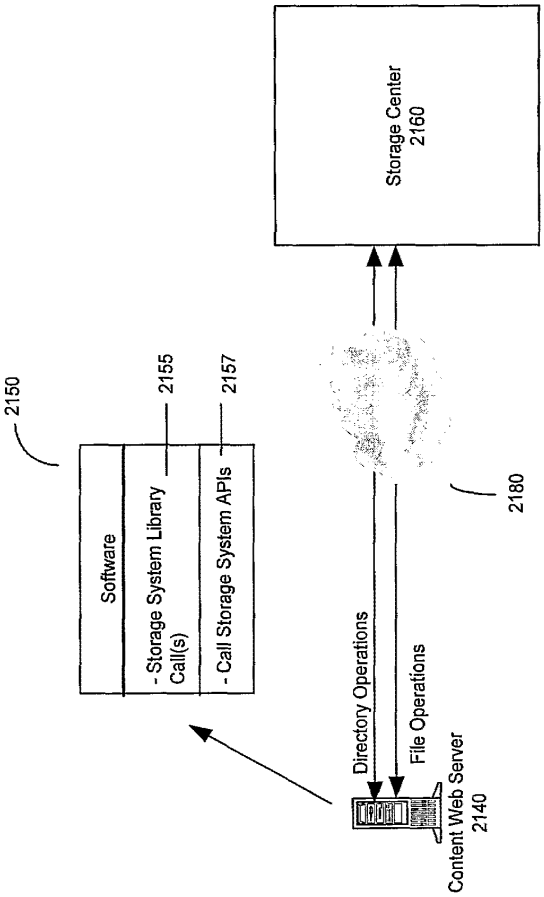


Figure 21b

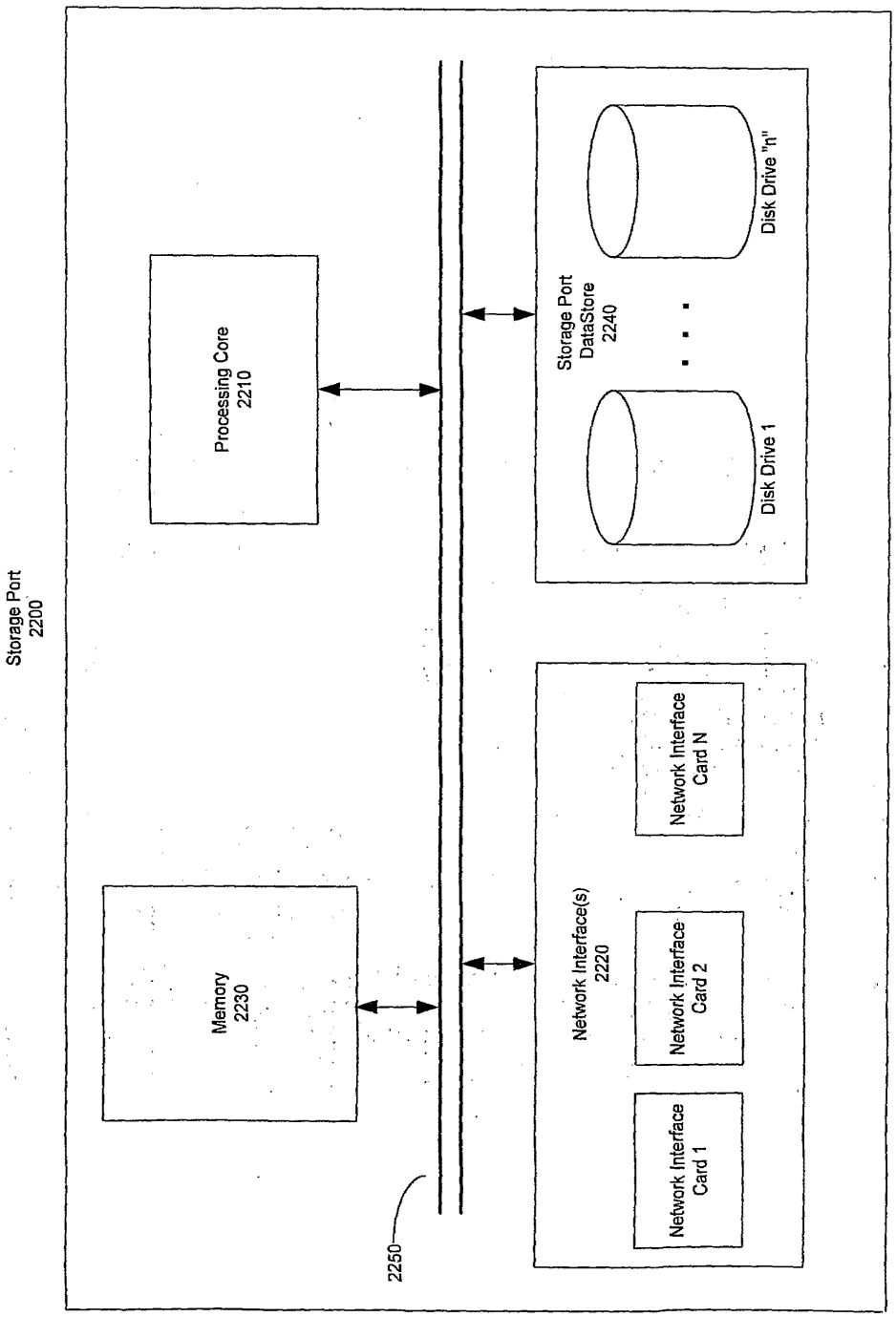

Storage Port
2200
Processing Core
2210
Memory
2230
2250
Network Interface(s)
2220
Network Interface
Card 1
Network Interface
Card 2
Network Interface
Card N
Storage Port
DataStore
2240
Disk Drive 1
Disk Drive "n"

Figure 22

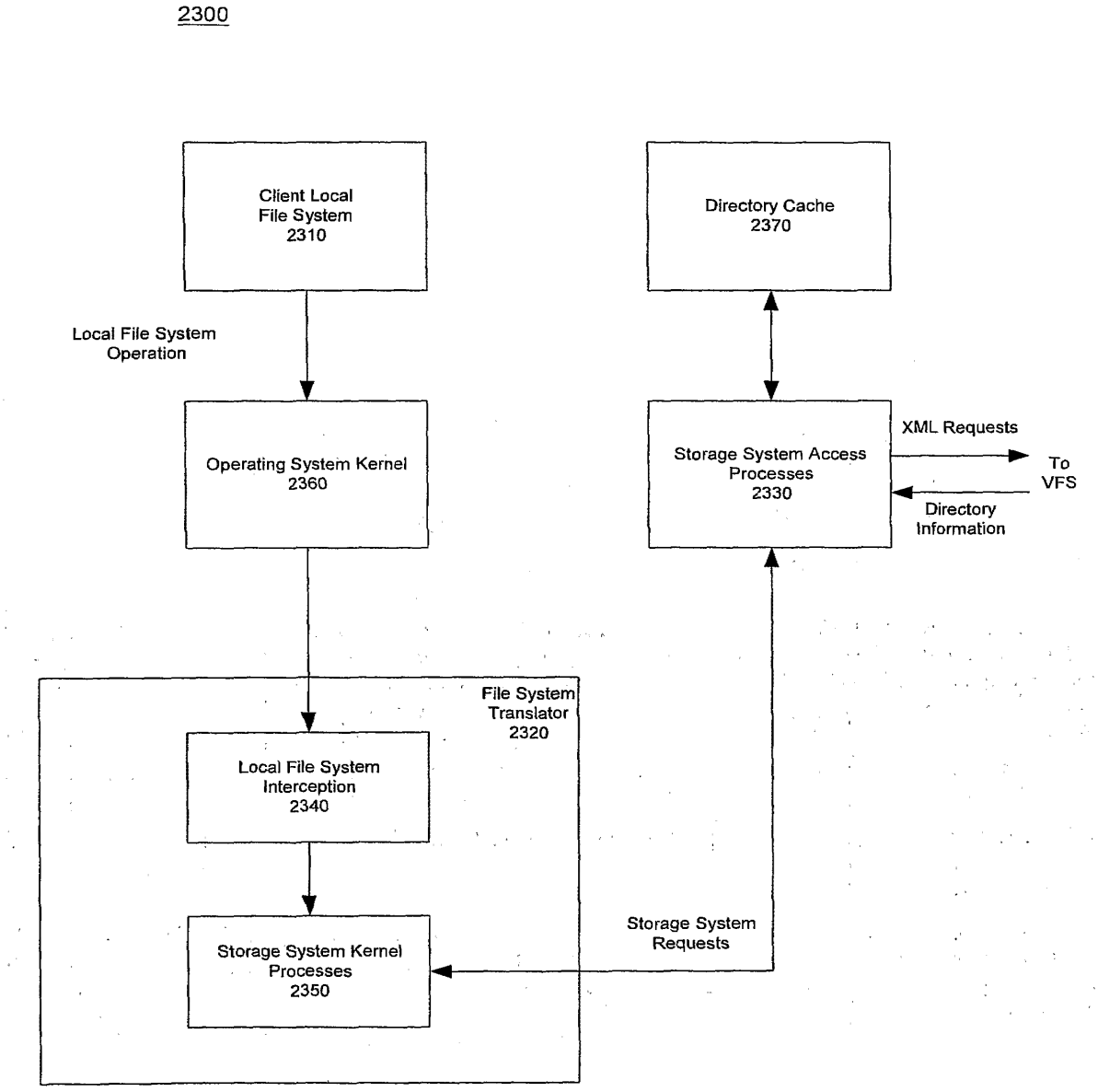

2300
Client Local File System 2310
Directory Cache 2370
Local File System Operation
Operating System Kernel 2360
Storage System Access Processes 2330
XML Requests
To VFS
Directory Information
File System Translator 2320
Local File System Interception 2340
Storage System Kernel Processes 2350
Storage System Requests

Figure 23

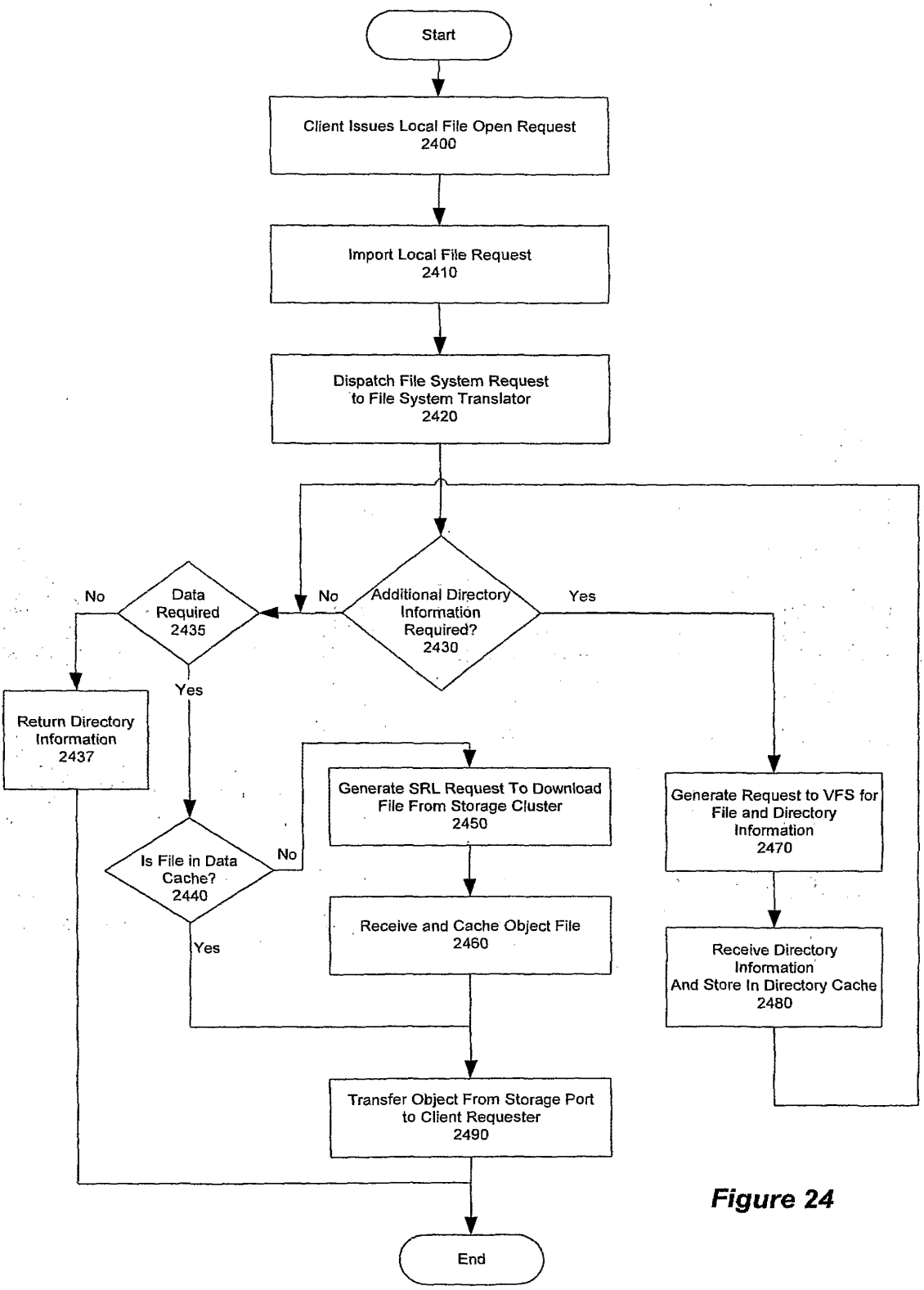

Start
Client Issues Local File Open Request
2400
Import Local File Request
2410
Dispatch File System Request
to File System Translator
2420
Additional Directory
Information
Required?
2430
No
Yes
Data
Required
2435
No
Yes
Return Directory
Information
2437
Is File in Data
Cache?
2440
No
Yes
Generate SRL 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

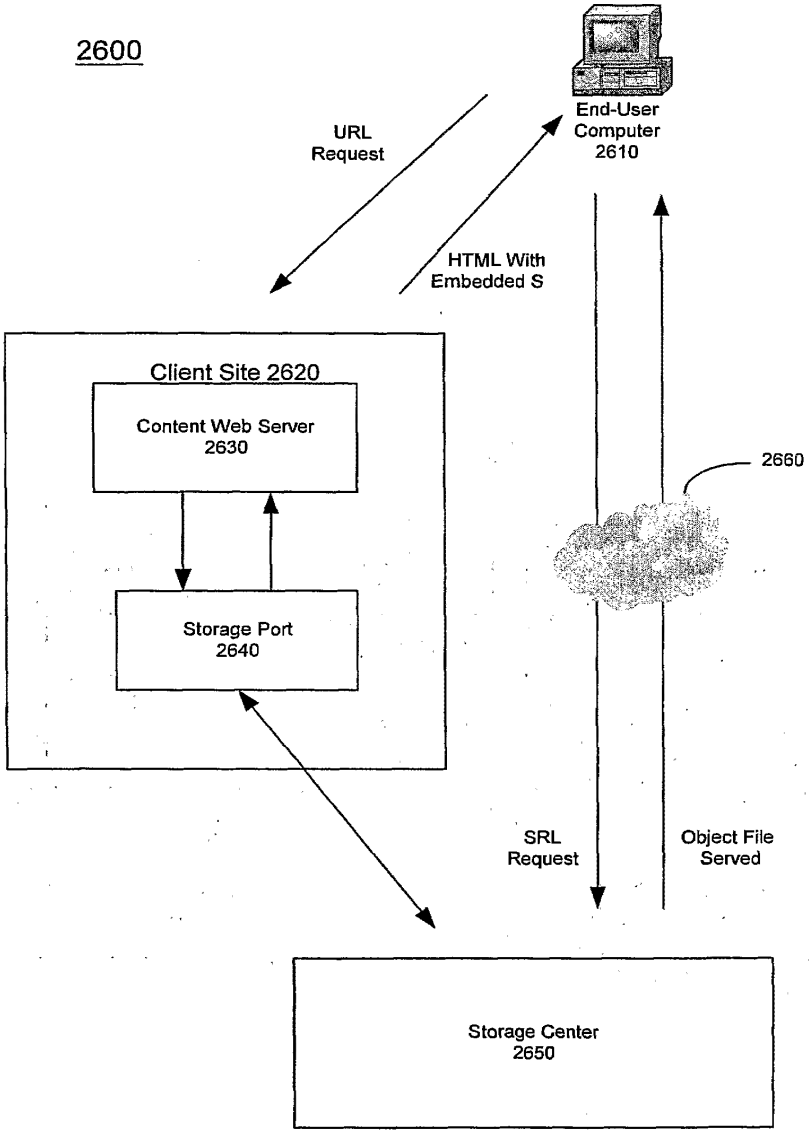

2600
End-User
Computer
2610
URL
Request
HTML With
Embedded S
Client Site 2620
Content Web Server
2630
Storage Port
2640
2660
SRL
Request
Object File
Served
Storage Center
2650

Figure 25

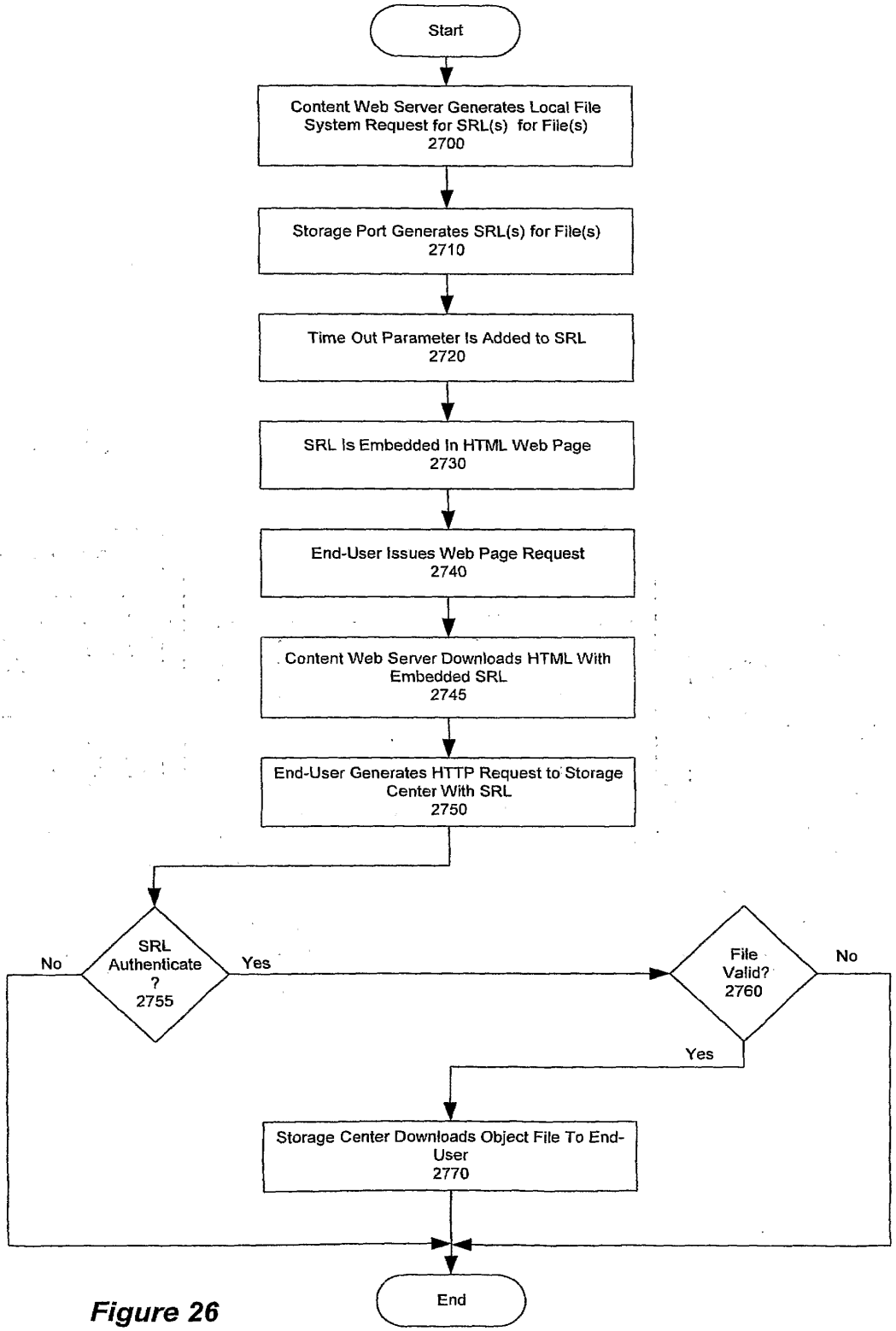

Start
Content Web Server Generates Local File System Request for SRL(s) for File(s) 2700
Storage Port Generates SRL(s) for File(s) 2710
Time Out Parameter Is Added to SRL 2720
SRL Is Embedded In HTML Web Page 2730
End-User Issues Web Page Request 2740
Content Web Server Downloads HTML With Embedded SRL 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

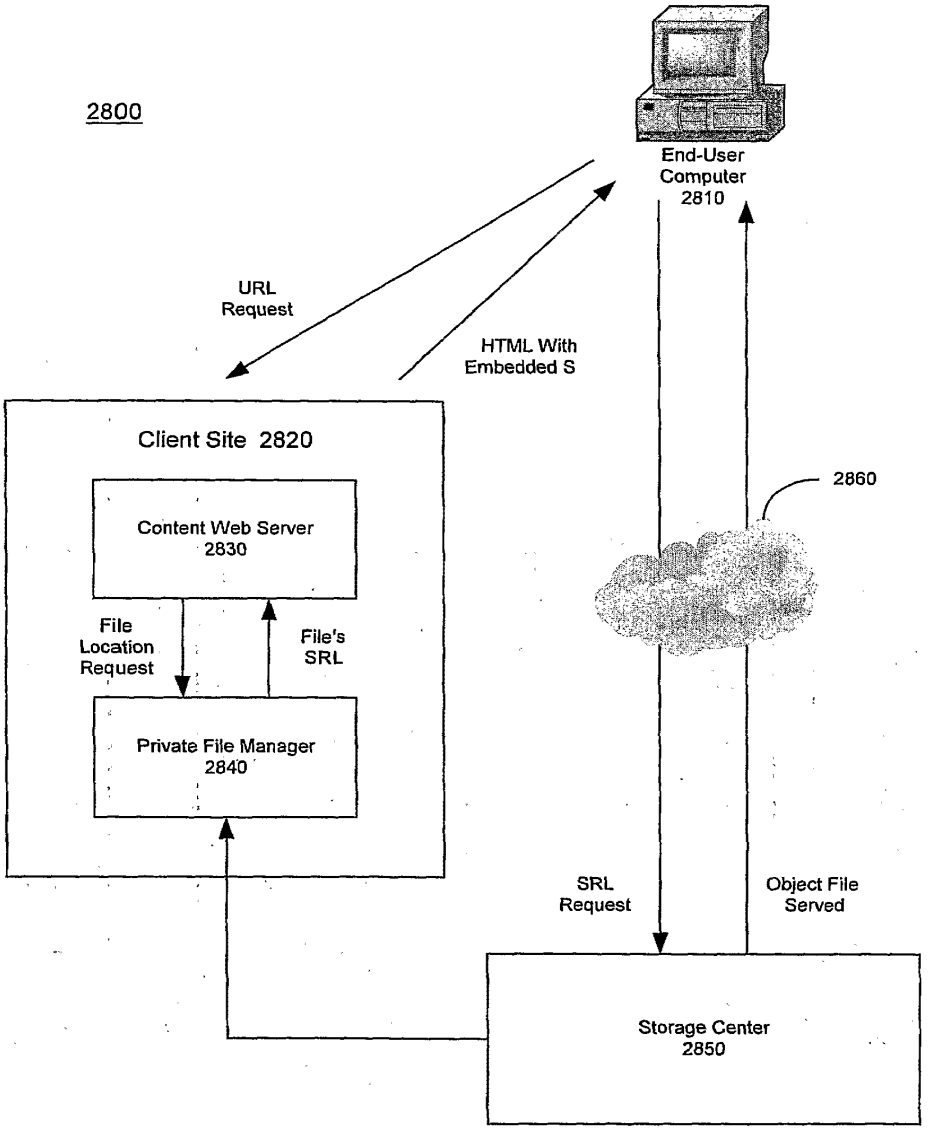

2800
End-User Computer 2810
URL Request
HTML With Embedded S
Client Site 2820
Content Web Server 2830
File Location Request
File's SRL
Private File Manager 2840
2860
SRL Request
Object File Served
Storage Center 2850

Figure 27

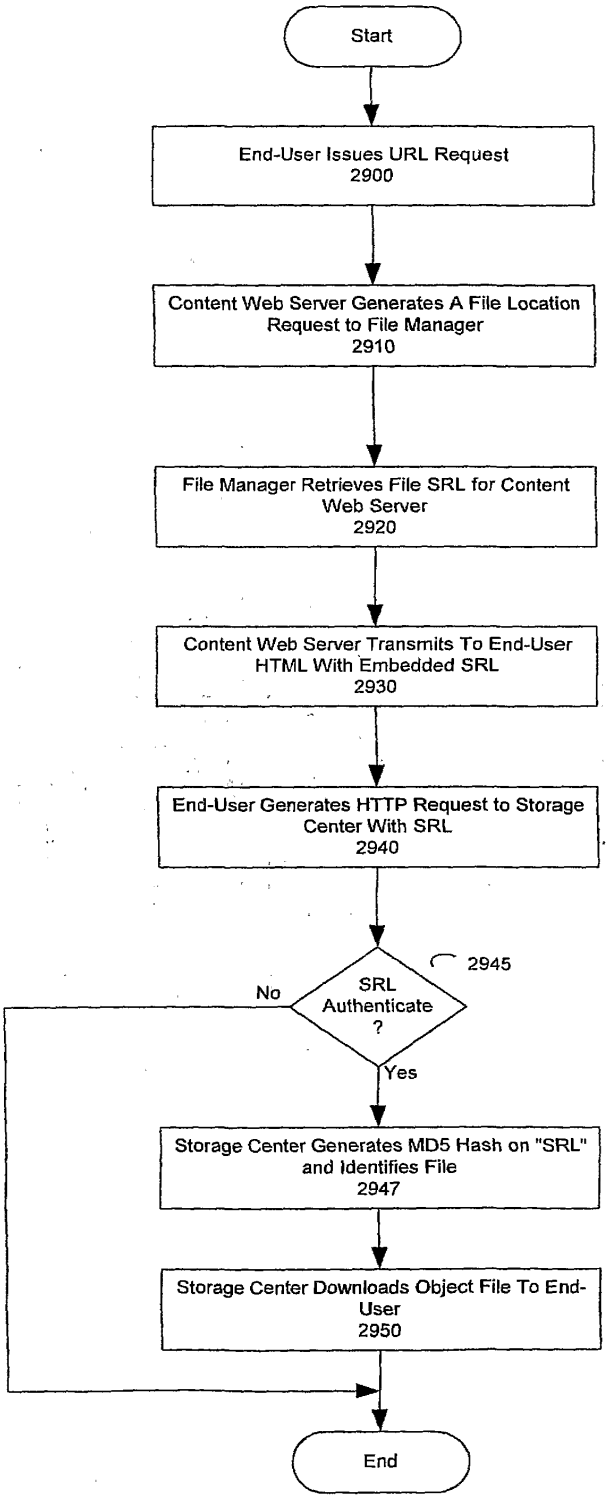

Start
End-User Issues URL Request
2900
Content Web Server Generates A File Location Request to File Manager
2910
File Manager Retrieves File SRL for Content Web Server
2920
Content Web Server Transmits To End-User HTML With Embedded SRL
2930
End-User Generates HTTP Request to Storage Center With SRL
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

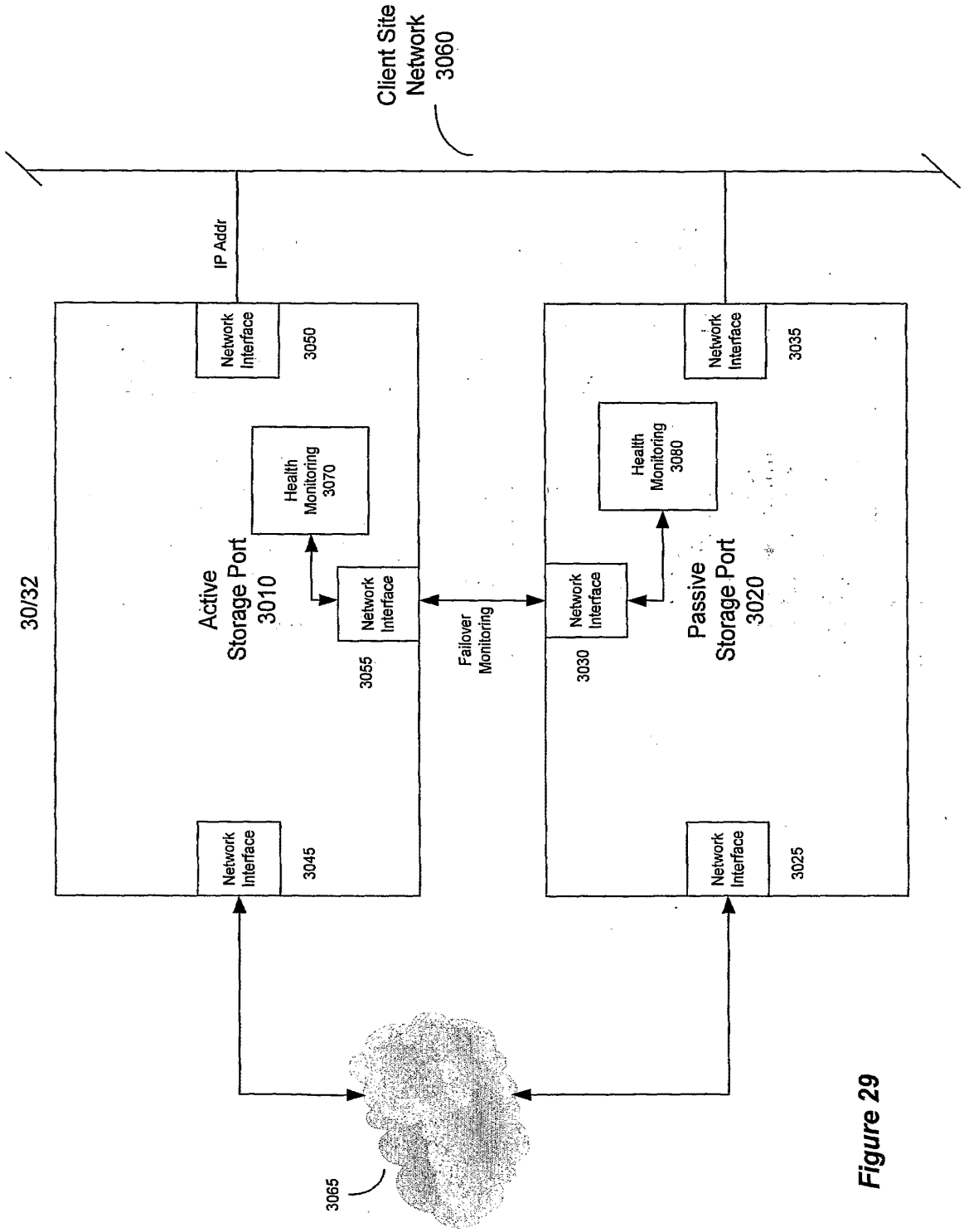

Client Site Network 3060
IP Addr
Network Interface
3050
Health Monitoring 3070
Active Storage Port 3010
Network Interface
3055
Failover Monitoring
Network Interface
3030
Health Monitoring 3080
Passive Storage Port 3020
Network Interface
3035
Network Interface
3045
Network Interface
3025
30/32
3065

Figure 29

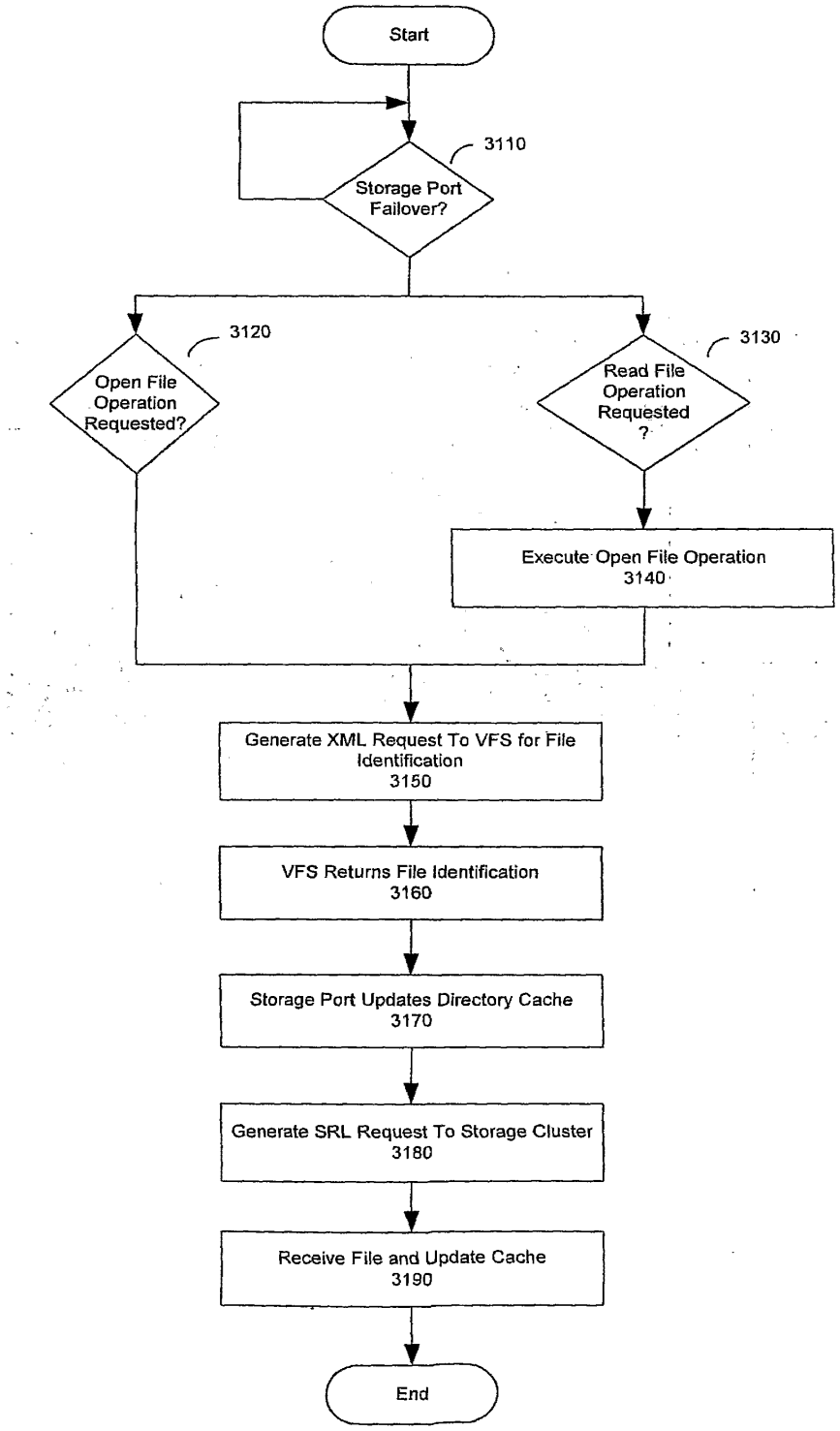

Start
3110
Storage Port Failover?
3120
Open File Operation Requested?
3130
Read File Operation Requested ?
Execute Open File Operation 3140
Generate XML Request To VFS for File Identification 3150
VFS Returns File Identification 3160
Storage Port Updates Directory Cache 3170
Generate SRL Request To Storage Cluster 3180
Receive File and Update Cache 3190
End

Figure 30

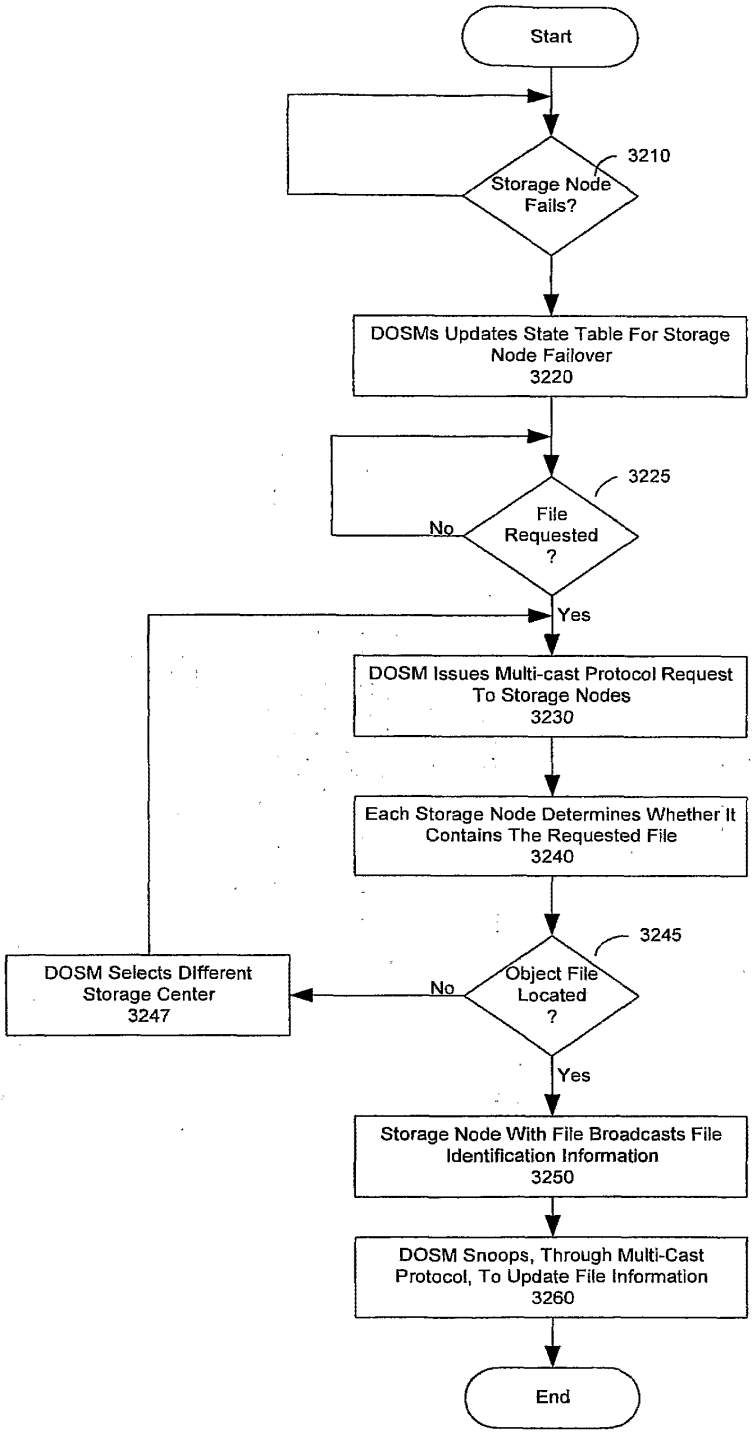

Start
3210
Storage Node Fails?
DOSMs Updates State Table For Storage Node Failover 3220
3225
File Requested ?
No
Yes
DOSM Issues Multi-cast Protocol Request To Storage Nodes 3230
Each Storage Node Determines Whether It Contains The Requested File 3240
3245
Object File Located ?
No
DOSM Selects Different 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**

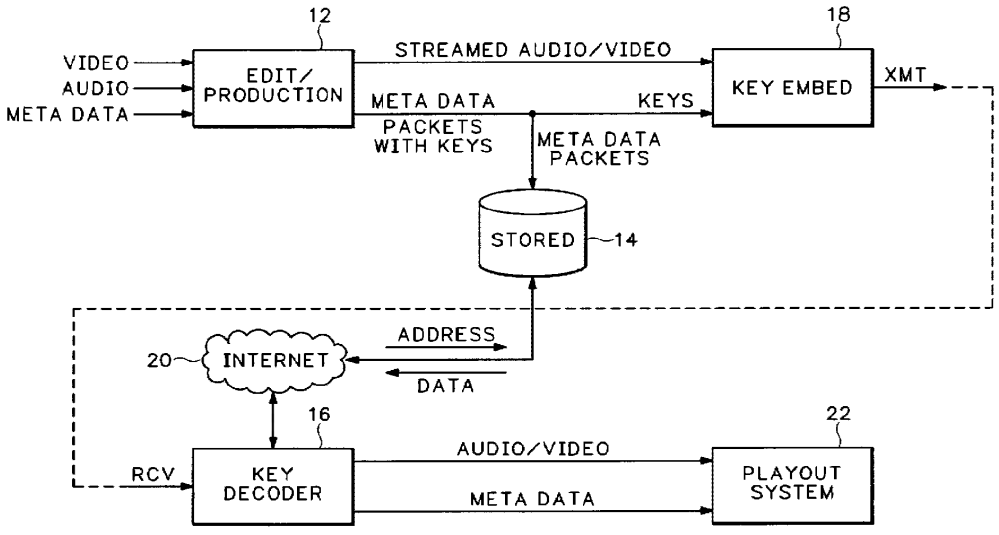
(71) Applicant: **Tektronix, Inc.**
Beaverton, OR 97077 (US)

(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 1254 of 1311
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

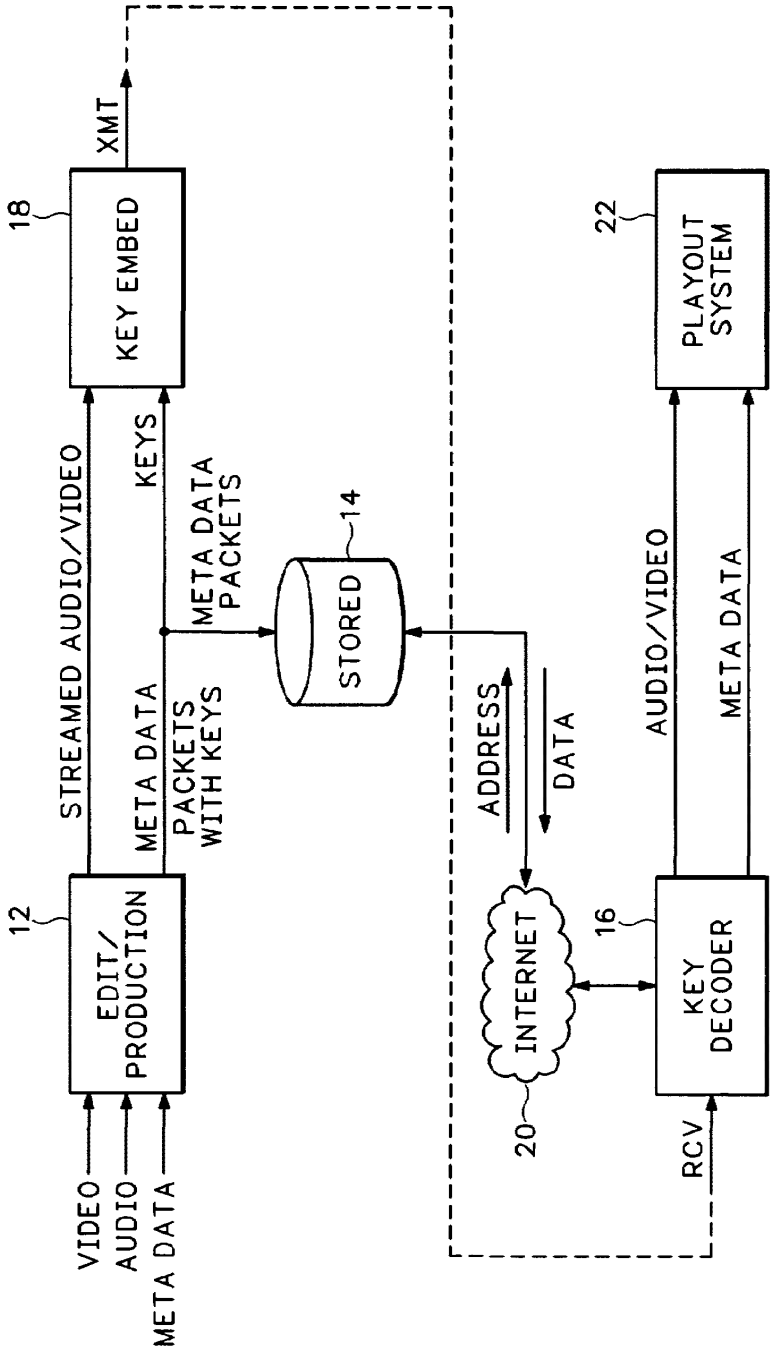
1. A method of synchronizing a data file with associated audio/video data using subliminally embedded keys comprising the steps of:

   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 1255 of 1311
APPLE INC.


XMT
18
KEY EMBED
22
PLAYOUT SYSTEM
STREAMED AUDIO/VIDEO
KEYS
META DATA PACKETS
14
STORED
AUDIO/VIDEO
META DATA
META DATA
PACKETS WITH KEYS
ADDRESS
DATA
12
EDIT/ PRODUCTION
INTERNET
16
KEY DECODER
20
VIDEO
AUDIO
META DATA
RCV

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/272,013

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	600
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*			OR	x 80 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 420 =	0.00
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).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1600

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	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 found in the appropriate box in column 1.

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
15/272,013	09/21/2016	2668	1600	MPOR-33317	20	2

CONFIRMATION NO. 8747

25883
HOWISON & ARNOTT, L.L.P
P.O. BOX 741715
DALLAS, TX 75374-1715

FILING RECEIPT

OC000000088209498

Date Mailed: 10/04/2016

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 14/660,166 03/17/2015
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 claims benefit of 60/757,075 01/06/2006
and is a CIP of 11/325,373 01/04/2006 PAT 7184573
which 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: 10/03/2016
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/272,013**
Projected Publication Date: 01/12/2017
Non-Publication Request: No
Early Publication Request: No
Title

METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, 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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
APPLICATION FOR UNITED STATES PATENT

METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL

Inventor:

MALONE, Michael F – McKinney, Texas

Attorneys:
Howison & Arnott, L.L.P.
P.O. Box 741715
Dallas, Texas 75374-1715

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a Continuation of U.S. Patent Application No. 14/660,166, filed March 17, 2015, and entitled METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL, which is a Continuation of U.S. Patent Application No. 13/965,625, filed August 13, 2013, and entitled METHOD FOR VOICE COMMAND ACTIVATION, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL, now U.S. Patent No. 8,983,119, issued on March 17, 2015 (Atty. Dkt. No. MPOR-31788). U.S. Patent Application No. 13/965,625 is a Continuation of U.S. Patent Application No. 13/417,229, filed on March 10, 2012, and entitled METHOD FOR MULTI-MEDIA CAPTURE, TRANSMISSION, CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL, now U.S. Patent No. 8,509,477, issued on August 13, 2013 (Atty. Dkt. No. MPOR-31064), the specifications of which are incorporated herein by reference.

[0002] U.S. Patent Application No. 13/417,229 is a Continuation of U.S. Patent Application No. 12/857,358, filed on August 16, 2010, and entitled METHOD FOR MULTI-MEDIA CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL, published as U.S. Patent Application Publication No. US 2010/0303288, now U.S. Patent No. 8,135,169, issued on March 13, 2012. U.S. Patent Application Publication No. 2010/0303288 and U.S. Patent No. 8,135,169 are incorporated by reference herein.

[0003] U.S. Patent Application No. 12/857,358 is a Continuation of U.S. Patent Application No. 11/621,062, filed on January 8, 2007, and entitled METHOD FOR MULTI-MEDIA RECOGNITION, DATA CONVERSION, CREATION OF METATAGS, STORAGE AND SEARCH RETRIEVAL, published as U.S. Patent Application Publication No. US 2007/0150517, now U.S. Patent No. 7,778,438, issued on August 17, 2010. U.S. Patent Application Publication No. U.S. 2007/0150517 and U.S. Patent No. 7,778,438 are incorporated by reference herein.

[0004] U.S. Patent Application No. 11/621,062 is a Continuation-in-Part of U.S. Patent Application No. 11/325,373, filed January 4, 2006, and entitled APPARATUS FOR CAPTURING INFORMATION AS A FILE AND ENHANCING THE FILE WITH EMBEDDED INFORMATION, published as U.S. Patent Application Publication No. US 2006/0115111, now U.S. Patent No. 7,184,573, issued on February 27, 2007. Application No. 11/621,062 claims benefit of U.S. Provisional Application No. 60/757,075, filed on January 6, 2006, and entitled APPARATUS AND METHOD FOR EMBEDDING META-TAGS INTO MEDIA FILES. U.S. Patent Application Publication No. US 2006/0115111 and U.S. Patent No. 7,184,573 are incorporated by reference herein.

[0005] U.S. Patent Application No. 11/325,373 is a Continuation of U.S. Patent Application No. 10/674,910, filed September 29, 2003, and entitled FORENSIC COMMUNICATION APPARATUS AND METHOD, published as U.S. Patent Application Publication No. US 2004/0125208, now U.S. Patent No. 6,996,251, issued on February 7, 2006. Application No. 10/674,910 claims benefit of U.S. Provisional Application No. 60/414,449, filed September 30, 2002, and entitled FORENSIC COMMUNICATION APPARATUS AND METHOD. U.S. Patent Application Publication No. US 2004/0125208 and 6,996,251 and U.S. Patent No. 6,996,251 are incorporated by reference herein.

TECHNICAL FIELD

[0006] This invention relates to the storage and search retrieval of all types of digital media files, whether music or other audio, still photographs, videos, movies or other types of media.

BACKGROUND

[0007] The popularity of digital media devices such as digital cameras, video cameras, mobile phones with audio and video recording capability and portable music devices that have recording capability has exploded in recent years. Instead of recording pictures, video and sound on physical media, modern devices record to rewritable memory devices. This means that the cost to create a new image, movie or audio recording has fallen to near zero, making the number of these recordings available in any given individual's library skyrocket.

[0008] But this new ability to store virtually unlimited numbers of media files introduces new problems. First, the sheer number makes it nearly impossible to manually describe and index every media file in one's possession. This means that, 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.

[0009] The second problem is the fact that people typically trade up to a new computer every three years or so. This means that hours of video, thousands of pictures or hundreds of audio files must be transferred from the old system to the new -- a sometimes daunting task.

[0010] A third problem is one can typically access locally stored media files only on the computer on which they reside. If one wishes to share the file with another one must typically employ some file-transfer method ahead of time (email, FTP, public server, etc.)

[0011] A fourth problem relates to e-mailing or sending your media files to another party, whereas the receiving party is not able to search the media files for the specific key indexes that the original owner had intended. While there are programs to allow the originator to type in key index words (tags) for searching and retrieving these media files from their personal computer, when these media files are e-mailed or sent to another party, these tags are removed from the media file, therefore the receiving party does not have an ability to search, sort, display, play or print these media files based on the original owners key indexes.

[0012] Finally, those who make a living providing content need some method for proving that a given work belongs to them, and that they are the original creator of the work.

SUMMARY

[0013] The present invention disclosed and claimed in one aspect thereof a system for capturing data in a first media and storing in a database at a remote location on a network. A network interface device is provided having a first capture device interfacing with a first external information source that generates external information and capturing the first external information during generation thereof. A processor is provided for processing the captured first external information and storing it in a first media format as stored first captured information within the network interface device, the processor initiating the storage of the first captured information as stored first captured information at an initial time and completes storage of the first captured information as stored first captured information at a completion time, thus providing a stored defined set of first captured information representing the first captured information between the initial time and the completion time. A transmitter is provided for transmitting as a transmitted defined set of first captured information the defined set of stored captured information to a remote location on a network after the completion time. A remote processing system is disposed at the remote node on the network and includes a database and a receiver for receiving the transmitted defined set of first captured information from the transmitter associated with the network interface device as a received defined set of first captured information. A data converter is operable to convert the received defined set of first captured information to a second format as a set of converted first captured information, the second format different than the first media format, the second format being a searchable format. The database then stores the set of converted captured information.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following description taken in conjunction with the accompanying Drawings in which:

[0015] Fig. 1 illustrates a block diagram of the overall operation of the system in accordance with the present disclosure.

[0016] Fig. 2 illustrates a block diagram of one embodiment of the overall operation of the system in accordance with the present disclosure.

[0017] Fig. 3 illustrates a block diagram of another embodiment of the overall operation of the system in accordance with the present disclosure.

[0018] Fig. 4 illustrates a block diagram of the file management of the system in accordance with the present disclosure.

DETAILED DESCRIPTION

[0019] Referring now to Fig. 1, there is illustrated a block diagram of the overall operation of the system in accordance with the present disclosure. The invention is best described by beginning with the capture device 100.

[0020] Still pictures, moving pictures, audio, telemetry or other information (hereafter called simply, "information") is gathered by the data converter 102 and organized into one "data element" 104 consisting of a single picture, a movie/video clip, an audio clip, a sample of telemetry data or other logical grouping of related information. The data converter 102 can be any type of data capture information. For pictures, a digital camera can be utilized and, for movie/video clips, the data converter can be a digital video recorder (DVR). In general, the data converter is any type of device that will capture the information and place it in some type of digitized format. As will be understood and discussed herein below, this digitized format is typically native to the data converter and the manufacturer. Some manufacturers have a particular file format in which they generate the information. This file format may have a designator as to the user, a sequence number or time stamp.

[0021] At the same time the data element is created by the capture device 100, certain other data ("meta data") 106 is captured as well. This meta data may include time and date 158, location 160, operator identification 162, or other information deemed relevant to establish the context of the data element. The time, date and location may be taken from a GPS unit, or may be derived by time-domain analysis of certain types of mobile phone signals or wireless network domains.

[0022] In some embodiments of this invention, it may be desirable to use a technique known as *steganography* to permanently and indelibly embed the meta data directly into the data element. By using one of several well-known steganographic techniques, the data element can be subtly altered such that 1) it is difficult to determine that hidden information is stored in the data element, and 2 even if it is known that hidden information is stored in the data element, retrieval without some secret information (a "key") is difficult. In this way, the data element can be guaranteed authentic even if stripped from external meta data.

[0023] Also, at the time of information capture, the capture device may gather additional information from the operator by means of a secondary data converter 108 that relates to defining the context of the data element. 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. This "context description element" 110 is stored along with the data element and the meta data.

[0024] At this point, the capture device 100 has in its internal temporary storage the data element, the meta data and optionally the context description element. It now creates a composite data set using one of a number of well-known algorithms for combining multiple data sets into a single data set. For example, the well-known ZIP compression algorithm routinely performs statistical compression on a number of input files and creates a single output file such that, with the proper decompression algorithm, the original set of files can be recovered without data loss. This "combine and compress" function 112 creates a data set called the "composite element." 114.

[0025] The capture device now encrypts the composite element using any of a number of well-known encryption algorithms. In the preferred embodiment, the composite element is first encrypted using a symmetrical cryptosystem 116 using a key 118 shared by the capture device and the storage facility. The resulting "singly-encrypted element" 120 is then hashed. "Hashing" 122 is a technique that generates a digital "signature" for a data set, such that any party wishing to verify the correctness of the data set can easily recalculate the hash and compares it with the previously calculated hash. Hash algorithms have the further property that it is computationally difficult to find multiple data sets that have the same hash value. This calculated hash value ("element hash") 124 becomes part of the meta data set that is to be associated with the data element.

[0026] It is now necessary for the capture device to contact the storage facility over some communications medium. This communications medium 126 can be any mechanism that permits near real-time, two-way communication. The specifics of the communication medium are not disclosed here, but could comprise a wireless telephone network, the public switched telephone network, or the Internet. The capture device sends the meta data 106 (now consisting of the time,

date, operator identification, image, video, audio, "context description element" 110, hash 122 and possibly other data) to the storage facility 128.

[0027] The storage facility validates the meta data received from the capture device and, if authorized, combines and hashes 130 the received meta data and a secret number 132 known only to the storage facility. This hash is appended to the original meta data set and is then returned to the capture device as a "certificate." 134 At a later time, the certificate can be presented to the storage facility to determine if a data element is authentic.

[0028] The singly encrypted element 120 is now combined with the certificate 134 and then is further encrypted using an asymmetrical cryptosystem 136 under the public encryption key 164 of the storage facility 128, designated K_{SU}. This new packet (the "transport packet") 138 is now ready to transmit to the storage facility 128.

[0029] When it receives the transport packet 138, the storage facility 128 first decrypts 140 the packet 138 using its private decryption key 166 designated as K_{SR}. This gives the storage facility 128 access to the certificate 134 (which contains the meta data 106). The certificate can be validated 142 by rehashing the meta data 106 and the secret number 132. Unpacking the certificate 134, the storage facility 128 now knows the identity of the capture device 100, and can use this to retrieve the secret, symmetrical key 118 under which the singly encrypted element 120 is encrypted. The storage facility 128 now decrypts 149) the singly encrypted element 120 to retrieve the composite element 114; then expands and recovers 150 the composite element to retrieve the data element 104, the meta data 106, and the context description element 110, if present.

[0030] Now, the storage facility 128 can store the data element 104 under the owner's account in its mass storage 144. The storage facility knows the owner's identity because it was disclosed in the meta data 106. The storage facility also adds "context tags" 146 by methods dependent on the type of data that is being stored.

[0031] Context tags 146 are searchable elements derived from either the data element 104 itself or from the context description element 110. For example, if the data element 104 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.

[0032] It is equipment analyze the data elements (photograph, movie, audio recording, etc.) and create 148 a set of appropriate tags. For audio files, this may include a speech-to-text algorithm; for still or moving images, it may include image recognition and identification. Whatever the method used, at the end of the process the set of data to store includes the data element 102, the context element 110, and meta data 106 that now includes a set of searchable tags specific to that image, video, audio or other media. 146, presumed that, as image and voice recognition improve; this task can be fully automated. Therefore, the preferred embodiment of this invention is to have the task automated.

[0033] Retrieval of the data elements is performed from some access point 152 remote from the storage facility 128. To retrieve data elements, a client must prove to the storage facility that the client is authorized to access the desired data element. This can be done in any number of ways, but in the preferred embodiment of the invention, it is a password challenge. The access point 152 creates an authentication request 154 and transmits the request via the communications medium 126 to the storage facility 128. At the storage facility, the request is authenticated 156. Once the challenge has been successfully met, the client can access the data elements belonging to it. Details of the authentication process may include password authentication, a challenge/response protocol, or may employ a hardware authentication device.

[0034] Once the request for information has been authenticated, the storage facility 128 reads the requested information from the bulk storage device 144 and encrypts 169) under the public key of the requester 168, designated as K_{CU}. The encrypted data is then transmitted to the client over the communications medium 126. Upon arrival, the message is decrypted 172 under the client's private key 170 designated as K_{CR} and the data 174 is recovered.

[0035] Once the data has been retrieved, the tags may be edited or removed and new tags added. Other meta data; particularly location and time and date cannot be changed.

[0036] Variations of the system include placing the ability to enter tags on the data capture device itself. This could be in the form of a keypad, a touch screen or voice recognition software. If this option were taken, the data packet from the image capture device would include the tags in the meta data rather than a context description element.

[0037] Another variation applies to highly secure applications in which it is desirable to keep the data element 104 encrypted even while at the storage facility. In this variation, the data element 104 is encrypted under a symmetrical cryptosystem prior to combination with the meta data 106 and the context description element 110. This variation precludes the automatic extraction of tags from the data element itself, but still permits tagging based on the context description element.

[0038] Referring now to Fig. 2, there is illustrated a diagrammatic view of the overall operation of the system. In this system, the capture device 100 is disclosed wherein the actual device that captured it, the device 102, is illustrated as being a digital camera. This has a lens 202 associated therewith, with the output of the camera being a digitized image 204. This is basically the data element 104 of Fig. 1. It can be seen that the element 204 is in a digitized format that is typically native to the camera. This can be any type of video capture element for capturing an image 206.

[0039] Once the image is captured, it is stored in a data base 208. In addition to this information, various associated information such as audio, timestamp, GPS, location, etc. can be collected. 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. This not only converts it to a digital value but, further, will convert it to a particular audio format such as a *.WAV file format. This particular file format is stored in the database 208. Of course, any other type of digital format could be utilized that is consistent with an audio format. The GPS information for location can be collected with an external GPS system 218 and timestamp information can internally be generated.

[0040] After all the information regarding the video information and the audio information, for example, is collected, it is stored in the database 208 and then must be output therefrom. In this embodiment, there are two types of attached information that are to be embedded within the image at a later time. The first set of information is the GPS information, the timestamp information, etc., that is collected automatically with any image. This information is created in a temporal relationship with respect to that particular image at the time of the capture of the image information. This location information, timestamp information, etc., is information that is unique to the photograph and defines that image. Further, user information can be provided which defines the user information that is associated with the capture device, i.e., the camera. The additional information, the audio information, is provided in the form of comments and the such which can be stored. Therefore, when the data in the form of the image information is to be transmitted to the remote site, it is combined with the additional GPS, location, timestamp, etc., information and the audio input information.

[0041] There is typically provided a unique file format that defines the digital image and this unique file name can be utilized to define all of the secondary information such that there is a unique association of that information with the image. Thereafter, a compress module 220 is provided for compressing the information in a compressed file format such as a *.ZIP file format. This is just a manner to transmit a number of files together. However, at the reception point, when the files are extracted from this *.ZIP file, there must be some way to distinguish the files and again associate them. This is done, for example, with a unique file naming structure. However, there could be other techniques utilized to uniquely identify the association between these different files.

[0042] Once this compressed file format is transmitted to the storage facility 128, it is stored in a database 226. 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. This, in effect, is a relational database that provides data storage in close association with each other. The first thing that must be done is to extract the information from the data. This is done in a block 228 wherein the associated information is extracted from the database, this being the associated information, and then processed. Typically, the associated information will be the

audio information in the audio file format. This must be converted. One conversion that is provided for is to convert the audio formatted data to text data. Therefore, one type of audio-to-text converter can be a voice translation system. There are many of these that are provided such as the Dragon Naturally Speaking systems.

[0043] Once the text format has been provided, this is a converted to intermediate formatted data, i.e., text data, that can then be processed in a format that can be embedded within a video file or an image file. This can then be converted into HTML data or other data. This will typically be formatted such that it can be defined as a meta tag for association with the video image. This meta tag is then combined with the image in a block 230. Once combined, this will then be stored in the database in association with the original raw video and raw audio files. Thereafter, there is an access and retrieval block 152 that can allow one to access the particular modified or "tagged" image via a search. There can be provided a search algorithm that searches all of the tagged images. This searching can be performed based upon the GPS location information, the timestamp information, the added audio comment information, etc. Any 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, as this is the information that is contained in the appended information to the image.

[0044] Referring now to Fig. 3, there is illustrated an alternate embodiment wherein substantially all of the combining operation is contained within the capture device 100 or the camera. Again, there is provided the capture device 102 in the form of the camera that captures the image 206. This is converted and stored in a database 306. The database 306 is basically the combination of database 208 and the database 226. Initially, all of the information from the digital video image 204 and the audio information and all other associated information such as the GPS information, timestamp, etc., are all stored in the database 306. There will be a corresponding process 308 for taking the associated information and converting it into different information, i.e., a meta tag, which is substantially the same as the process 228. Once the associated process is combined it is converted into that format, then it can be combined with the image in a process block 310, similar to the process block 230. Once this occurs, then there is provided a combined video/image with meta data that can be transmitted. This is illustrated as

the augmented image 316 which has meta data associated therewith. This is transmitted for storage at the storage facility in a database 318. This is searchable through the access/retrieval process 152, as described herein above.

[0045] Referring now to Fig. 4, there is illustrated one exemplary embodiment of the file structure. The image 204 is a digitized image that constitutes a particular file folder that will have a particular video or image format. This could be a JPEG format, an MPEG format or any other type of video format. This is referred to as one having the extension *.VID (for generic purposes). The file format in this embodiment will have a user ID section 402, a time/date stamp section 404, a sequence number 406 and a device number 408. This will have the format of XXX.AAAA.XXX.XXX.VID. The user ID section 402 will define the user of the capture device, this typically being configuration information that is input to the system. The time/date stamp is time and date information that can be taken from an internal clock or it can be derived from some external accurate time source. The sequence number 406 is typically internally generated with a counter that represents an internal sequence that is unique to a particular capture device. However, among different capture devices, the sequence could be the same. The device section 408 is a unique device number given to a particular device. Therefore, with the user ID information, the time/date stamp, the sequence number and the device number, a very unique file number will be generated. Further, the sequence and the time/date information will be different for each file. Thereafter, the information retrieved from the GPS 218 will be disposed in a folder with an extension of, for example, *.GPS. This will be stored in the file folder 208. The file numbering will be identical to the file nomenclature other than the extension will be identical to that of the digitized video file. Similarly, the audio information will be stored in a file folder with an extension of, for example, *.WAV with the body of the file name being identical to that of the digitized video file. This will all be stored in the database 208 and then combined in a compressed folder of the *.ZIP type. The actual file name for this can be any type of file name and it does not have to be identical or unique with respect to the name. However, there should be some type of unique file name in that, a random filename could be duplicated by other capture devices. Thus, in the preferred embodiment of this disclosure, the unique body of the *.ZIP file will be identical to that associated with the files contained therein such that this will have a filename of "XXX.AAAA.XXX.XXX.ZIP." This is the file that is transmitted.

[0046] As a summary, the system of the present disclosure provides a system for capturing, storing, indexing and retrieving data objects, which can include a capture device, a storage facility and an access point. The system consists of a primary data converter, a secondary data converter, a meta data source, a data combiner and compressor, a symmetrical encryptor, a one-way hash function, an asymmetric encryptor, and a communications port. The primary data converter captures some physical phenomenon such as, but not limited to a still image, a moving image, a sound, or some other factor, into a primary data set. The secondary data converter is capable of capturing some phenomenon into a secondary data set, related to but separate from the information captured by the primary data converter. The meta data source produces a device identifier, time, date, location, and other data related to the information captured by the primary data converter into a meta data set. The source of the time, date and location information is a GPS receiver, a wireless receiver or another receiver. The source of the device identifier is a read-only memory device. The data combiner and compressor is capable of combining the output of the multiple sources of data (the primary data converter, the secondary data converter, and the meta data source) into a single data stream, and then compressing said data stream into a compressed data set such that the compressed data set requires fewer transmission or storage resources than the uncompressed stream, but remains recoverable such that the original data from the primary data converter, the secondary data converter and the meta data source can be recovered without error. The symmetrical encryptor is capable of using a key shared with another party to convert the data stream from the data combiner and compressor into a singly encrypted data set that is unusable by any party other than the party that has knowledge of the key. The one-way hash function is capable of calculating for the encrypted data stream from the symmetric encryptor a number associated with said data stream such that (a) the number represents the data stream, but the data stream is not recoverable from the number, and (b) that it is computationally infeasible to created a second data stream that, when presented to the one-way hash function, produces an identical number. The communications port is capable of sending the meta data and the hash to a second party. The communications port is further capable of receiving from a second party a certificate that has the property of (a) being uniquely and verifiably identified with the meta data and hash of claim 12, and (b) being verifiably identified as originating with the second party. The asymmetric encryptor is capable of converting the output of the symmetric encryptor and other data into an encrypted information packet that can

be read only by a specific second party by means of a pair of related but non-identical keys, the encryption key and the decryption key. The communications port is further capable of conveying the encrypted information packet to a second party. The storage facility consists of a communications port, a device authenticator, an asymmetric decryptor, a validator, a symmetric decryptor, a data expander and recovery device, a tag generator, a mass storage mechanism, an asymmetric encryptor, and a user authenticator. The communications port is capable of receiving a request from validation from the capture device. The device authenticator is capable of verifying that the capture device is authorized to use the storage facility and to create an authentication certificate such that (a) it is computationally infeasible to create a second meta data set or hash that creates an identical authentication record, and (b) the authentication record is uniquely identified with the storage facility. The asymmetric encryptor is capable of using the decryption key to recover the authentication certificate and the singly encrypted data set. The validator is capable of determining if the recovered authentication certificate (a) was generated by the storage facility, and (b) is valid for the presented hash and meta data. The symmetric decryptor is capable of converting the singly encrypted data set into the compressed data set. The data expander and recovery device is capable of converting the compressed data set into the original primary data set, the secondary data set, and the meta data set. The tag generator is capable of taking the primary data set, the secondary data set and the meta data set and producing a set of index tags that describe the primary data set. The tag generator in which the tag generation is performed by a human operator. The tag generation is performed by a speech-to-text function or by an image recognizer. The mass storage mechanism is capable of storing the primary data set, the secondary data set and the meta data set in a way that the information can be retrieved based on the index tags. The user authenticator is capable of receiving requests from access points and verifying their authority to perform retrieval operations at the storage facility.

[0047] The system can, at its most condensed version, comprise an asymmetric encryptor capable of converting data read from the mass storage mechanism using a public encryption key into a form usable only by a party with knowledge of a secret key that corresponds to the said public encryption key. The access point consists of an asymmetric decryptor, a communications port and an authentication requester. The authentication requester is capable of identifying the

access point and the data element or elements to be recovered from the storage facility in a manner that proves its authority to access said data element or elements.

WHAT IS CLAIMED IS:

1. A system for capturing data in a first media and storing in a database at a location on a network, comprising:

a capture device having:

a first data converter interfacable with a first external information source that generates external information and the first data converter capturing the first external information during generation thereof,

the first data converter processing the captured first external information and storing it in a first media format as stored first captured information within the capture device, the first data converter initiating the storage of the first captured information as stored first captured information at an initial time and completing storage of the first captured information as stored first captured information at a completion time, thus providing a stored defined set of first captured information representing the first captured information between the initial time and the completion time, and

a transmitter for transmitting as a transmitted defined set of first captured information the defined set of stored captured information to the location on the network after the completion time;

a system disposed at the location on the network and including:

a database,

a receiver for receiving the transmitted defined set of first captured information from the transmitter associated with the capture device as a received defined set of first captured information,

a system data converter for converting the received defined set of first captured information to a second format as a set of converted first captured information, the second format different than the first media format, the second format being a searchable format, and

the database storing the set of converted captured information.

2. The system of Claim 1, and further comprising:

a second data converter in the capture device for interfacing with a second external information source to capture second external information therefrom;

the second data converter processing the captured second external information and storing it in a third format different from the first media format as stored second captured information;

a combiner for associating the defined set of stored first captured information with the stored second captured information;

the transmitter transmitting the associated defined set of stored first captured information and stored second captured information to the location on the network;

the receiver at the system receiving the transmitted defined set of stored first captured information and stored second captured information form the transmitter;

the database storing the set of converted captured information with the associated stored second captured information such that the association of the defined set of stored first captured information and stored second captured information is maintained.

3. The system of Claim 2, wherein the second external information is temporal and is complete as to the capture at the time of capture by the second data converter.

4. The system of Claim 2, wherein the third format is a second media format different from the first media format and wherein the third format of a second media format is maintained in the database at the location on the network.

5. The system of Claim 1, wherein the second data converter captures information from the second external information source indicative of the location of the capture device and the second data converter processing the second captured information for storage as location information as the stored second captured information.

6. The system of Claim 5, and further comprising an other data capture device in the capture device that comprises a Global Positioning System (GPS) device.

7. The system of Claim 5, and further comprising an other data capture device in the capture device that derives location information from a time domain analysis of mobile phone signals.

8. The system of Claim 5, and further comprising an other data capture device in the capture device that derives location information from a time domain analysis of wireless network domains.

9. The system of Claim 5, and further comprising an other data capture device in the capture device that derives location information from Doppler analysis of timing signals from cellular/PCS base stations.

10. The system of Claim 5, wherein the capture device comprises a cell based communication device and further comprising an other data capture device in the capture device that captures location information as to cell transmitters and the other data capture device in the capture device that determines location information from cell triangulation.

11. The system of Claim 2, wherein the first data converter comprises an audio transducer and the first media format comprises a format representing audio information.

12. The system of Claim 11, wherein the second format of the converted set of first captured information represents text.

13. The system of Claim 1, wherein the first data converter comprises an audio transducer and the first media format comprises a format representing audio information.

14. The system of Claim 13, wherein the second format of the set of converted first captured information represents text.

15. The system of Claim 1, wherein the capture device comprises a portable handheld device.

16. The system of Claim 1, the capture device has stored thereat a first capture device identifier and the transmitter transmitting the first capture device identifier with the associated defined set of stored first captured information and stored second captured information to the remote location.

17. The system of Claim 1, and further comprising an encryptor for encrypting at least a portion of the defined set of stored captured information transmitted by the transmitter at some time between the completion time and the receipt by the system.

18. The system of Claim 1, wherein the encryptor encrypts the defined set of stored captured information proximate in time to the completion time.

19. The system of Claim 1, wherein the encryptor encrypts at a first level of encryption as an encrypted file that constitutes a symmetrical encryption algorithm that has a secret key available only to an owner of the defined set of stored captured information and wherein the encrypted file is placed in combination with the owner information in the transmission and wherein the system is operable to store the received information.

20. A system for capturing data in a first media for storage in a database at a location on a network, comprising:

a capture device having:

a first data converter interfacable with a first external information source that generates external information and capturing the first external information during generation thereof,

a second data converter interfacing with a second external information source to capture second external information therefrom at an instant in time;

the first data converter processing the captured first external information from a start event representing the time that capture is initiated to a stop event representing the time that capture is complete and storing it in a first media format as a stored defined set of first captured information within the capture device, the second data converter for processing the captured second external information and

storing it as second captured information and a combiner for generating an association between the defined set of first captured information and the second captured information, and

a transmitter for transmitting the associated stored defined set of first captured information and second captured information as a transmitted associated defined set of first captured information and second captured information to the location on the network after at least stop event associated with the associated with the processing of the captured second external information;

a system disposed at the location on the network and including:

a database,

a receiver for receiving the transmitted associated defined set of first captured information and second captured information from the transmitter associated with the capture device as a received set of first captured information,

a system data converter for converting the received defined set of first captured information to a second format as a set of converted first captured information, the second format different than the first media format, the second format being a searchable format, and

the database storing the set of converted captured information in association with the associated received second set of captured information.

ABSTRACT

This invention relates to a network interface device. A first capture device interfaces with a first external information source to capture first external information. A processor processes the captured first external information and stores it in a first media. The processor initiates the storage of the first captured information at an initial time and completes storage of the first captured information at a completion time, thus providing a stored defined set of first captured information. A transmitter transmits the defined set of stored captured information to a remote location on a network. A remote processing system is disposed at the remote node on the network and includes a database and a receiver for receiving the transmitted defined set of first captured information. A data converter is operable to convert the received defined set of first captured information to a second format. The database stores the set of converted captured information.

1/4

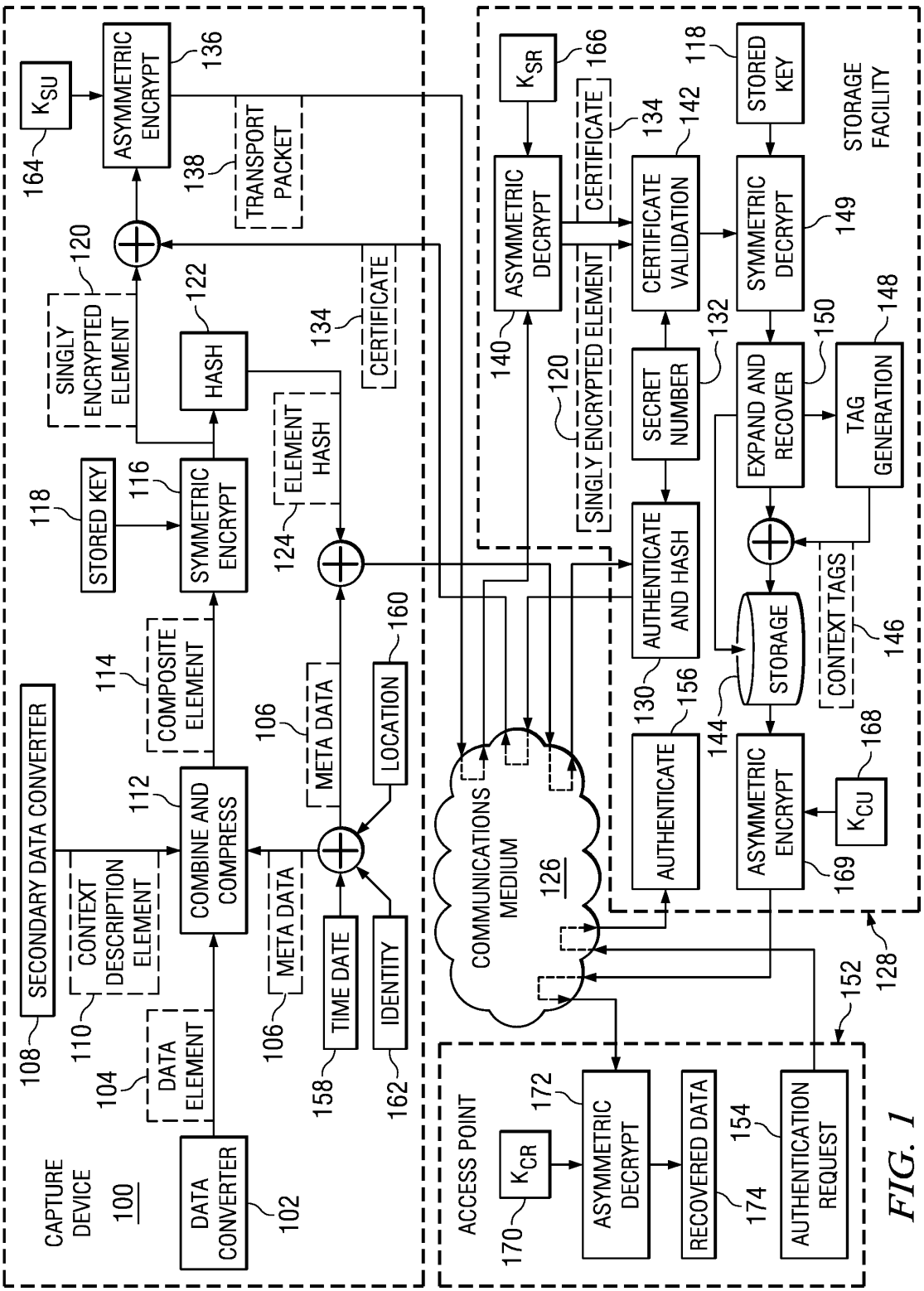

CAPTURE DEVICE
100
DATA CONVERTER
102
SECONDARY DATA CONVERTER
108
DATA ELEMENT
104
CONTEXT DESCRIPTION ELEMENT
110
COMBINE AND COMPRESS
112
COMPOSITE ELEMENT
114
SYMMETRIC ENCRYPT
116
STORED KEY
118
SINGLY ENCRYPTED ELEMENT
120
HASH
122
ELEMENT HASH
124
CERTIFICATE
134
ASYMMETRIC ENCRYPT
136
TRANSPORT PACKET
138
K_{SU}
164
META DATA
106
TIME DATE
158
IDENTITY
162
LOCATION
160
META DATA
106
COMMUNICATIONS MEDIUM
126
ACCESS POINT
K_{CR}
170
ASYMMETRIC DECRYPT
172
RECOVERED DATA
174
AUTHENTICATION REQUEST
154
152
128
STORAGE FACILITY
K_{SR}
166
ASYMMETRIC DECRYPT
140
CERTIFICATE
134
CERTIFICATE VALIDATION
142
STORED KEY
118
SYMMETRIC DECRYPT
149
SECRET NUMBER
132
EXPAND AND RECOVER
150
TAG GENERATION
148
SINGLY ENCRYPTED ELEMENT
120
AUTHENTICATE AND HASH
130
CONTEXT TAGS
146
STORAGE
144
AUTHENTICATE
156
ASYMMETRIC ENCRYPT
169
K_{CU}
168

FIG. 1

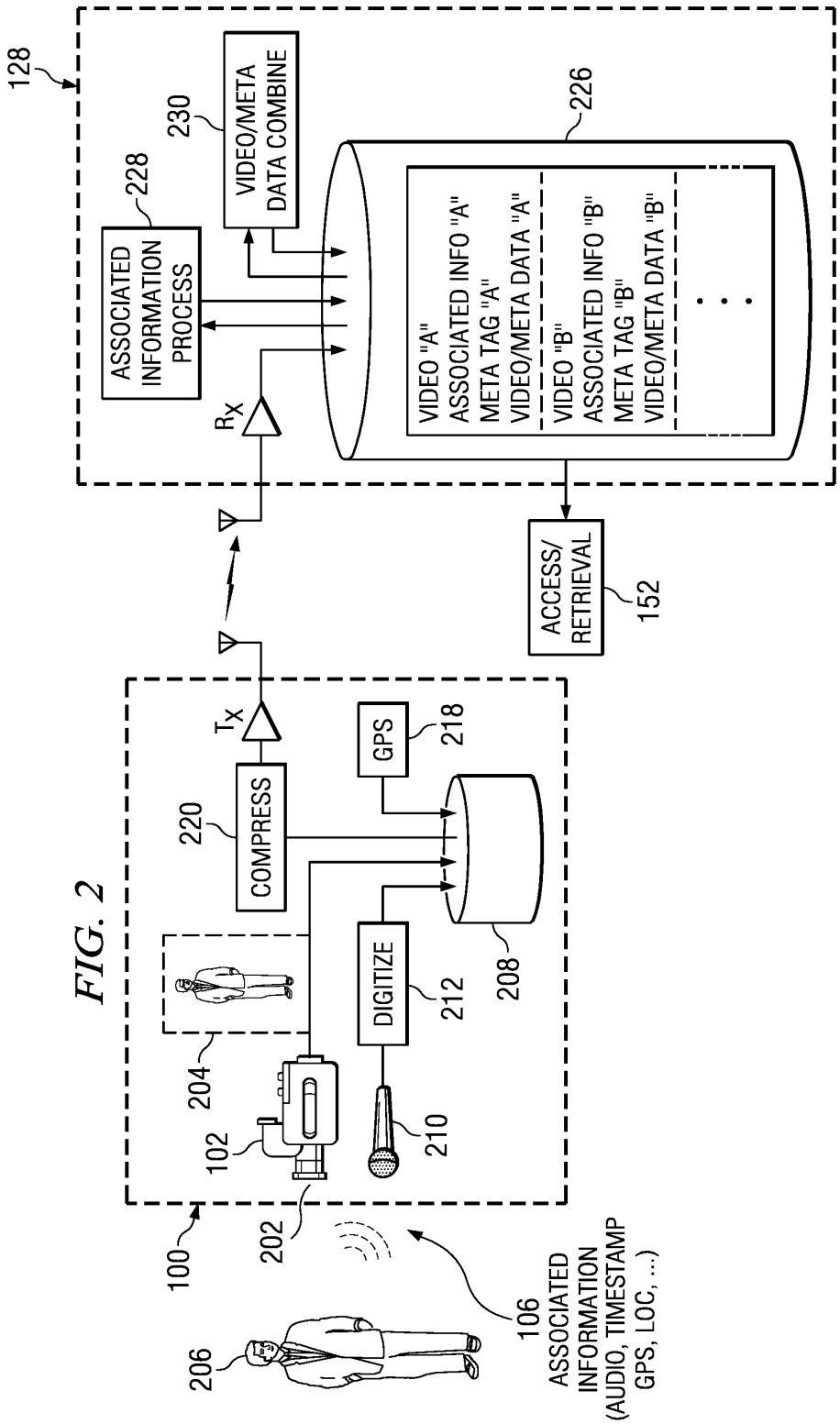

128
230
VIDEO/META DATA COMBINE
228
ASSOCIATED INFORMATION PROCESS
226
Rx
VIDEO "A"
ASSOCIATED INFO "A"
META TAG "A"
VIDEO/META DATA "A"
VIDEO "B"
ASSOCIATED INFO "B"
META TAG "B"
VIDEO/META DATA "B"
ACCESS/ RETRIEVAL
152
Tx
GPS
218
220
COMPRESS
208
DIGITIZE
212
204
102
210
100
202
206
106
ASSOCIATED INFORMATION (AUDIO, TIMESTAMP GPS, LOC, ...)

FIG. 2

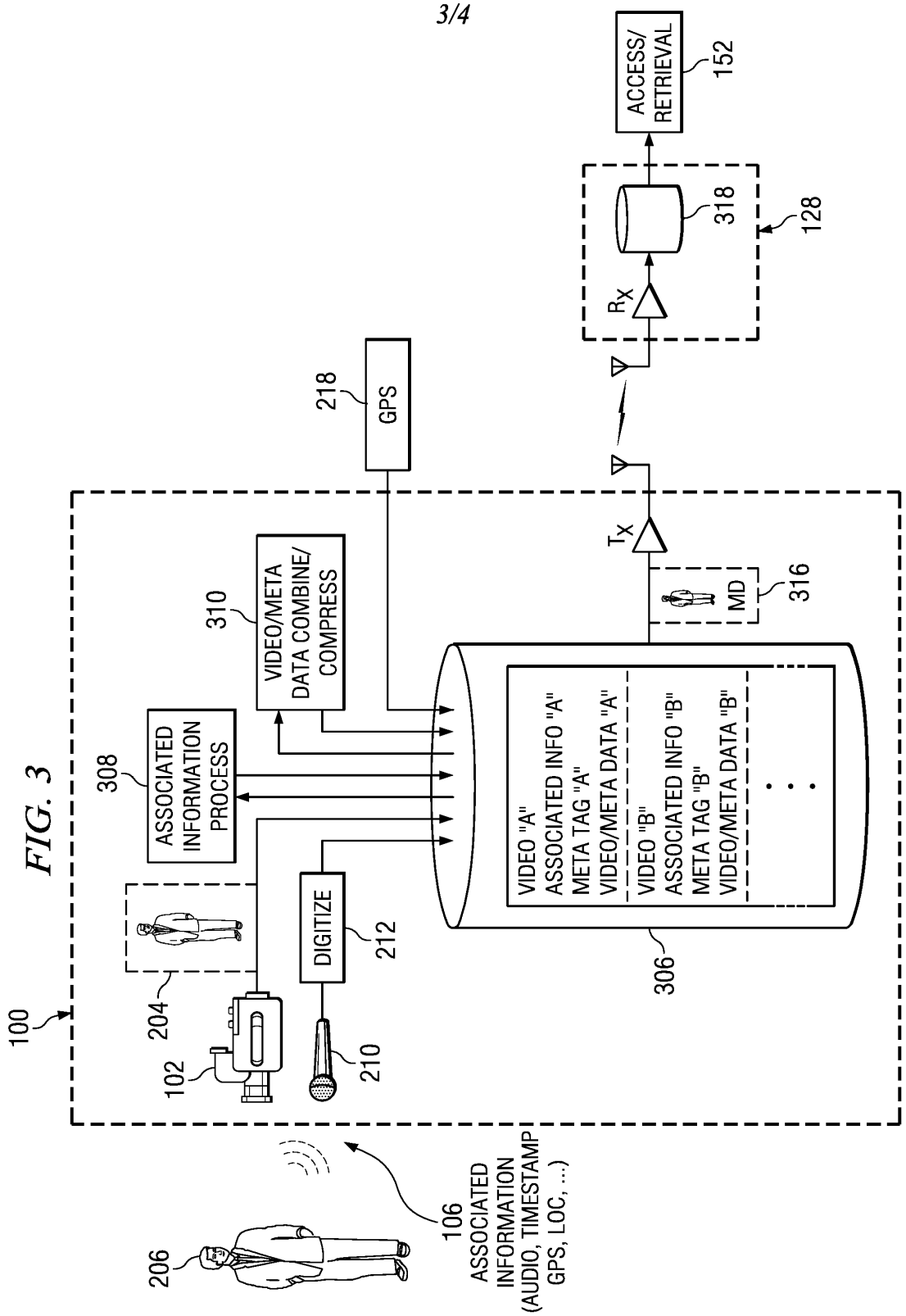

100
102
204
206
106
ASSOCIATED INFORMATION (AUDIO, TIMESTAMP GPS, LOC, ...)
210
DIGITIZE
212
308
ASSOCIATED INFORMATION PROCESS
310
VIDEO/META DATA COMBINE/ COMPRESS
218
GPS
Tx
Rx
MD
316
306
VIDEO "A"
ASSOCIATED INFO "A"
META TAG "A"
VIDEO/META DATA "A"
VIDEO "B"
ASSOCIATED INFO "B"
META TAG "B"
VIDEO/META DATA "B"
318
128
ACCESS/ RETRIEVAL
152

FIG. 3

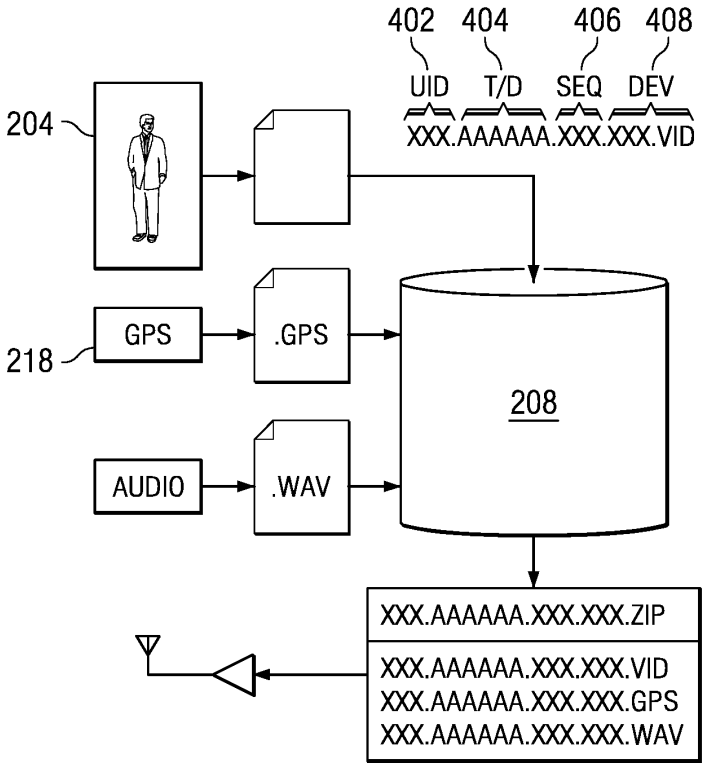

402
404
406
408
UID
T/D
SEQ
DEV
XXX.AAAAAA.XXX.XXX.VID
204
GPS
218
.GPS
208
AUDIO
.WAV
XXX.AAAAAA.XXX.XXX.ZIP
XXX.AAAAAA.XXX.XXX.VID
XXX.AAAAAA.XXX.XXX.GPS
XXX.AAAAAA.XXX.XXX.WAV

FIG. 4

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MPOR-33317
	Application Number	
Title of Invention	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 — Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	MICHAEL	F.	MALONE	

Residence Information (Select One) ● US Residency Non US Residency Active US Military Service

City	State/Province	Country of Residence
McKinney	TX	US

Mailing Address of Inventor:

Address 1	2711 Northview Drive
Address 2	

City	State/Province	Postal Code	Country
McKinney	TX	75070	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	25883		
Email Address	ADMIN@DALPAT.COM	Add Email	Remove Email

Application Information:

Title of the Invention	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL		
Attorney Docket Number	MPOR-33317	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)		**Suggested Figure for Publication (if any)**	

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MPOR-33317
	Application Number	
Title of Invention	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	US Patent Practitioner	◯ Limited Recognition (37 CFR 11.9)
Customer Number	25883		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	14/660166	2015-03-17

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MPOR-33317
	Application Number	
Title of Invention	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL	

Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14/660166	Continuation of	13/965625	2013-08-13	8983119	2015-03-17
Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13/965625	Continuation of	13/417229	2012-03-10	8509477	2013-08-13
Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13/417229	Continuation of	12/857358	2010-08-16	8135169	2012-03-13
Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12/857358	Continuation of	11/621062	2007-01-08	7778438	2010-08-17
Prior Application Status	Expired			Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
11/621062	Claims benefit of provisional	60/757075	2006-01-06		
Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
11/621062	Continuation in part of	11/325373	2006-01-04	7184573	2007-02-27
Prior Application Status	Patented			Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
11/325373	Continuation of	10/674910	2003-09-29	6996251	2006-02-07
Prior Application Status	Expired			Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
10/674910	Claims benefit of provisional	60/414449	2002-09-30		
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.				Add	

Foreign Priority Information:

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MPOR-33317
	Application Number	
Title of Invention	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL	

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MPOR-33317
	Application Number	
Title of Invention	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MPOR-33317
	Application Number	
Title of Invention	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	MYPORT TECHNOLOGIES, INC.		
Mailing Address Information For Applicant:			
Address 1	2711 Northview Drive		
Address 2			
City	McKinney	**State/Province**	TX
Country	US	Postal Code	75070
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MPOR-33317
	Application Number	
Title of Invention	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Keith D. Harden, Reg. #74472/			Date (YYYY-MM-DD)	2016-09-21
First Name	Keith	Last Name	Harden	Registration Number	74,472

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	MPOR-33317
	Application Number	
Title of Invention	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL	

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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 records.

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 CooperationTreaty.

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.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. 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.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	METHOD FOR VOICE COMMAND ACTIVATION, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

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 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.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Michael E. MALONE Date (Optional): 8/12/13

Signature: _____

Note: An application data sheet (PTO/AIA/14 or equivalent), including naming the entire inventive entity, must accompany this form. Use an additional PTO/SB/AIA01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1 minute 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.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL
First Named Inventor/Applicant Name:	Michael F. Malone
Filer:	Keith D. Harden
Attorney Docket Number:	MPOR-33317

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	280	280
UTILITY SEARCH FEE	1111	1	600	600
UTILITY EXAMINATION FEE	1311	1	720	720
Pages:				
Claims:				
Miscellaneous-Filing:				
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	1600

Electronic Acknowledgement Receipt	
EFS ID:	26995243
Application Number:	15272013
International Application Number:	
Confirmation Number:	8747
Title of Invention:	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, 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:	MPOR-33317
Receipt Date:	21-SEP-2016
Filing Date:	
Time Stamp:	17:10:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1600
RAM confirmation Number	4409
Deposit Account	200780
Authorized User	Harden, Keith
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 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		MPO33317CONTApp.pdf	157112 0e77cd40d2d72b19c9082a318f1a2f6e856d3792	yes	24
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	18	
	Claims		19	23	
	Abstract		24	24	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	MPO33317DWGS.pdf	226007 e8947bfb4b40ac636c45084e2558fd66367ce063	no	4
Warnings:					
Information:					
3	Application Data Sheet	MPO33317ADS.pdf	1823876 e5beb62152419 4aaa8270ce553e116beca77aaf0	no	9
Warnings:					
Information:					
4	Oath or Declaration filed	MPO33317DECEXE.pdf	145527 efd29a8ad6d088bda92fd9c7864a6c0f1d48ca3f	no	1
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	36711 d64810a7deffcf8eedeefd02e396190c29bb6832	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	2389233

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.

Electronic Acknowledgement Receipt	
EFS ID:	26995243
Application Number:	15272013
International Application Number:	
Confirmation Number:	8747
Title of Invention:	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, 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:	MPOR-33317
Receipt Date:	21-SEP-2016
Filing Date:	
Time Stamp:	17:10:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1600
RAM confirmation Number	4409
Deposit Account	200780
Authorized User	Harden, Keith
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 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		MPO33317CONTApp.pdf	157112 0e77cd40d2d72b19c9082a318f1a2f6e856d3792	yes	24
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	18	
	Claims		19	23	
	Abstract		24	24	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	MPO33317DWGS.pdf	226007 e8947bfb4b40ac636c45084e2558fd66367ce063	no	4
Warnings:					
Information:					
3	Application Data Sheet	MPO33317ADS.pdf	1823876 e5beb62152419 4aaa8270ce553e116beca77aaf0	no	9
Warnings:					
Information:					
4	Oath or Declaration filed	MPO33317DECEXE.pdf	145527 efd29a8ad6d088bda92fd9c7864a6c0f1d48ca3f	no	1
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	36711 d64810a7deffcf8eedeefd02e396190c29bb6832	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	2389233

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.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	15/272,013
Filing Date	September 21, 2016
First Named Inventor	Michael F. MALONE
Title	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, STORAGE AND SEARCH RETRIEVAL
Art Unit	
Examiner Name	
Attorney Docket Number	MPOR-33317

SIGNATURE of Applicant or Patent Practitioner

Signature	/Keith D. Harden, Reg. #74472/	Date (Optional)	
Name	Keith D. Harden	Registration Number	74,472
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of ONE forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. 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 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.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 25883

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

MYPORT TECHNOLOGIES, INC.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	
Name	Michael F. MALONE		
Title	CEO		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ Total of ONE forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. 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 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.

Electronic Acknowledgement Receipt	
EFS ID:	26996142
Application Number:	15272013
International Application Number:	
Confirmation Number:	8747
Title of Invention:	METHOD FOR PERSONAL VOICE ASSISTANT, LOCATION SERVICES, MULTI-MEDIA CAPTURE, TRANSMISSION, SPEECH CONVERSION, METATAGS CREATION, 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:	MPOR-33317
Receipt Date:	21-SEP-2016
Filing Date:	
Time Stamp:	17:21:56
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	Power of Attorney	MPO33317POAEXE.pdf	1481738 b65a8a21e118ae4a4b42643e5353f77d6fbf3f86	no	2

Warnings:

Information:	
Total Files Size (in bytes):	1481738

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.