IW 8176856

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

November 29, 2021

THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS OF:

APPLICATION NUMBER: *09/626,044*
FILING DATE: *July 27, 2000*
PATENT NUMBER: *6,757,828*
ISSUE DATE: *June 29, 2004*

By Authority of the
Under Secretary of Commerce for Intellectual Property
and Director of the United States Patent and Trademark Office

W. MONTGOMERY
Certifying Officer

JC862 U.S. PTO 09/626044 07/27/00

ISSUE CLASSIFICATION	Class	Subclass
	713	176

PATENT NUMBER 6757828

6757828

U.S. UTILITY Patent Application

O.I.P.E.	PATENT DATE
SCANNED LR ① Q.A. CH	JUN 29 2004 JUN 29 2004

APPLICATION NO.	CONT/PRIOR	CLASS	SUBCLASS	ART UNIT	EXAMINER
09/626044		713	176	2766 2135	Sons

APPLICANTS
Jonathan Jaffe
Joel Goldhar
Michael Warot

TITLE
Indigenous authentication for sensor-recorders and other information capture devices

PTO-2040 12/99

ISSUING CLASSIFICATION

ORIGINAL CLASS	ORIGINAL SUBCLASS	CROSS REFERENCE(S) CLASS	CROSS REFERENCE(S) SUBCLASS (ONE SUBCLASS PER BLOCK)					
713	176	380	200	258				

INTERNATIONAL CLASSIFICATION

H	0	4	L	9/00							

☐ Continued on Issue Slip Inside File Jacket

526604 Formal Drawings (21 sheets) not 1 7-27-00

☐ TERMINAL DISCLAIMER	DRAWINGS			CLAIMS ALLOWED	
	Sheets Drwg.	Figs. Drwg.	Print Fig.	Total Claims	Print Claim for O.G.
	21	21	1	6	1

☐ The term of this patent subsequent to _____ (date) has been disclaimed.

☐ The term of this patent shall not extend beyond the expiration date of U.S Patent. No. _____

Hasuk Sons (Assistant Examiner) 4/6/04 (Date)

(Primary Examiner) 4/19/04 (Date)

NOTICE OF ALLOWANCE MAILED 4/20/04

ISSUE FEE

Amount Due	Date Paid
$ 665.00	4/26/04 EBW

☐ The terminal ____ months of this patent have been disclaimed.

K. Watson Sanders 4/21/04 (Legal Instruments Examiner) (Date)

ISSUE BATCH NUMBER

WARNING:
The information disclosed herein may be restricted. Unauthorized disclosure may be prohibited by the United States Code Title 35, Sections 122, 181 and 368. Possession outside the U.S. Patent & Trademark Office is restricted to authorized employees and contractors only.

Form PTO-436A (Rev. 6/99)

FILED WITH: ☐ DISK (CRF) ☐ FICHE ☐ CD-ROM
(Attached in pocket on right inside flap)

ISSUE FEE IN FILE

(FACE)

SERIAL NUMBER	FILING DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/328,080	06/08/99	522	1711	265280-64159

APPLICANT

DONALD E. MCNULTY, WARSAW, IN; TODD SMITH, FORT WAYNE, IN.

CONTINUING DOMESTIC DATA********
VERIFIED SMC Provisional app # 60/088,729 June 10, 1998

371 (NAT'L STAGE) DATA********
VERIFIED
SMC

FC VIGN APPLICATIONS********
VERIFIED
SMC

IF REQUIRED, FOREIGN FILING LICENSE GRANTED 07/09/99

Foreign Priority claimed 35 USC 119 (a-d) conditions met	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐yes ☐no ☐yes ☒no ☐Met after Allowance Verified and Acknowledged SMC (Examiner's Initials) _____ (Initials)	IN	0	20	2

ADDRESS

~~BARNES & THORNBURG~~
~~11 SOUTH MENIDIAN STREET~~
~~INDIANAPOLIS IN 46204~~

Barry E. Bretschneider
Morrison & Foerster LLP
2000 Pennsylvania Ave NW
Washington DC 20006-1888

TITLE

CROSS-LINKED MOLDED PLASTIC BEARINGS

FILING FEE RECEIVED		
$760	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT NO. _____ for the following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

07-28-00

Please type a plus sign (+) inside this box → +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
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.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	6468/78445
First Inventor or Application Identifier	*Jonathan E. Jaffe et al.*
Title	INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES
Express Mail Label No.	EL045292082US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231

1. ☒ *Fee Transmittal Form (e.g. PTO/SB/17) (Submit an original and a duplicate for fee processing)

2. ☒ Specification (preferred arrangement set forth below) Total Pages 36
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure

3. ☒ Drawing(s) *(35 U.S.C. 113)* Total Sheets 21

4. Oath or Declaration Total Pages 4
   a. ☒ Newly executed (original or copy)
   b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d)) *(for continuation/divisional with Box 16 completed)*
      i. ☐ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

5. ☐ Microfiche Computer Program *(Appendix)*

6. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. ☐ Computer Readable Copy
   b. ☐ Paper Copy (identical to computer copy)
   c. ☐ Statement verifying identify of above copies

*NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

ACCOMPANYING APPLICATION PARTS

7. ☐ Assignment Papers (cover sheet & document(s))
8. ☐ 37. C.F.R. § 3.73(b) Statement *(when there is an assignee)* ☐ Power of Attorney
9. ☐ English Translation Document *(if applicable)*
10. ☐ Information Disclosure Statement (IDS) PTO-1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☒ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. ☒ *Small Entity Statement(s) *(PTO/SB/09-12)0* ☐ Statement filed in Prior application, Status still proper and desired
14. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. ☐ Other: _____

16. If a **CONTINUING APPLICATION**, *check appropriate box, and supply the requisite information below and in a preliminary amendment*

☐ Continuation ☐ Divisional ☐ Continuation-In-Part (CIP) Of prior application No.: _____/_____

Prior application information: Examiner _____ Group/Art Unit: _____

FOR CONTINUATION or DIVISIONAL APPS ONLY: The entire disclosure of the prior application, from which an oath or declarations supplied Under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by Reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

☐ *Customer Number or Bar Code Label* [ ] or ☒ *Correspondence address below*

Name	Jeffrey W. Salmon, Esq.				
	Welsh & Katz, Ltd.				
Address	120 S. Riverside Plaza				
	22nd Floor				
City	Chicago	State	Illinois	Zip Code	60606
Country	US	Telephone	(312) 655-1500	Fax	(312) 655-1501
Name *Print/Type)*	Daniel M. Gurfinkel			Registration No. *(Attorney/Agent)*	34,177
Signature				Date	July 27, 2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Office, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

07/27/00 JC862 U.S. PTO 09/626044

07/27/00 JC853 U.S. PTO

I hereby certify that this paper is being deposited with the United States Postal Service as Express Mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on this date.

Date

Express Mail Label No.

EL045920824S

PTO/SB/17 (12/99)
Approved for use through 09/30/00. OMB 0651-0032
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.

FEE TRANSMITTAL for FY 2000

Patent fees are subject to annual revision.
Small Entity payments must be supported by a small entity statement, otherwise large entity fees must be paid. See Forms PTO/SB09-12. See 37 C.F.R. § 1.27 and 1.28

TOTAL AMOUNT OF PAYMENT ($) 345.00

Complete if Known	
Application Number	Not yet assigned
Filing Date	July 27, 2000
First Named Inventor	*Jonathan E. Jaffe et al.*
Examiner Name	Not yet assigned
Group/Art Unit	Not yet assigned
Attorney Docket Number	6468/78445

07/27/00 JC662 U.S. PTO 09/626044

METHOD OF PAYMENT (check one)

1. ☒ The Commissioner is hereby authorized to charge indicated fees and credit any over payments to:

Deposit Account Number: 23-0920
Deposit Account Name: WELSH & KATZ, LTD.

☐ Charge any Additional Fee Required Under 37 CFR. 1.16 and 1.17

2. ☒ Payment Enclosed: ☒ Checks ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	690	201	345	Utility filing fee	345.00
106	310	206	155	Design filing fee	
107	480	207	240	Plant filing fee	
108	690	208	345	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 345.00

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below		Fee Paid
Total Claims	8	-20**=	0	x	9	=	0
Independent Claims	2	-3** =	0	x	39	=	0
Multiple Dependent Claims					130	=	0

**or number previously paid, if greater; For Reissues, see below

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	78	202	39	Independent claims in excess of 3
104	260	204	130	Multiple dependent claim
109	78	209	39	Reissue independent claims over original patent
110	18	210	9	Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) -0-

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge-late filing fee or oath	
127	50	227	25	Surcharge-late provisional filing fee or cover sheet	
139	130	139	130	Non-English Specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	380	216	190	Extension for reply within second month	
117	870	217	435	Extension for reply within third month	
118	1,360	218	680	Extension for reply within fourth month	
128	1,850	228	925	Extension for reply within fifth month	
119	300	219	150	Notice of Appeal	
120	300	220	150	Filing a Brief in support of an appeal	
121	260	221	130	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,210	241	605	Petition to revive - unintentional	
142	1,210	242	605	Utility issue fee (or reissue)	
143	430	243	215	Design issue fee	
144	580	244	290	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	690	246	345	Filing a submission after final rejection (37 CFR § 1.129(a)	
149	690	249	345	For each additional invention to be examined (37 CFR § 1.129(b)	

Other fee (specify) _____

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid **SUBTOTAL (3)** ($) -0-

SUBMITTED BY

Complete *(if applicable)*

Name *(Print/type)*	Daniel M. Gurfinkel	Registration No. *(Attorney/Agent)*	34,177	Telephone	(312) 655-1500
Signature				Date	July 27, 2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, D.C. 20231.

deposited with the United States Postal Service as Express Mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on this date.

Billie Chambers

Date

Express Mail Label No.

EL045892082US

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

08/07/2000 DBUTLER 00000014 09626044
01 FC:201 345.00 OP

PTO-1556
(5/87)

*U.S. GPO: 1999-459-082/19144

INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES

Field of the Invention

The present invention generally relates to a method and apparatus for acquiring and recording a sample of an environment and, more particularly, to a method and apparatus that allows the stored recording to be verified as an authentic, unaltered sample of the environment.

Background of the Invention

One purpose of the present invention is to provide a solution to the problem of either deliberate or inadvertent alteration of recordings. In this context, "recordings" refers to all recordings, including digital images, data files, and the more common audio recording.

Photographs, movies and printed materials have historically been regarded as media that can be trusted to be authentic copies of the original. Early attempts at alteration of photographs for the purposes of revisionist history were almost comically detectable with five people sitting at a table, but six pairs of legs underneath. Hand written, permanently bound, notebooks are used in research laboratories for their resistance against attempts at alteration. Recent technological advances have brought the ability to alter images to the neophyte level. When a master employs the advanced technology the alterations are almost completely undetectable. For this reason digital photography is seldom used in situations when "chain of custody" requirements exist to protect the authenticity of a recording be it photographic, written or auditory. For example, the picture of an accident scene could be altered to show bottles of alcoholic beverages around the driver, even if those bottles hadn't really been there when the picture was taken, but were a post accident embellishment.

...sited with the United States Postal Service as Express Mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on this date.

Date

Express Mail Label No.
EL045292082US

A digital camera with apparatus for authentication of images produced from an image file is disclosed in U.S. Patent No. 5,499,294. Referring to Fig. 3A of U.S. Patent No. 5,499,294, a block diagram of a system including a digital camera is shown that produces a file image with a digital signature. A device specific decryption key is required to allow a file image to be authenticated. Furthermore, in order to determine whether a file image is authentic, the person performing the authentication must know which camera took the picture; due to the fact that each camera includes a unique private encryption key.

Summary of the Invention

It is desirable to provide an improved method and system for determining the authenticity of a sample of an environment. A digital signature is created that is a function of both the sample of the environment itself, as well as at least one parameter that is representative of at least one condition under which the digital sample was acquired. The sample is stored in memory together with the at least one parameter and the digital signature. Authenticity of the stored image is determined by creating a new signature from the stored image and at least one parameter, and then comparing the two signatures to determine if they are the same.

Such a method and apparatus is advantageous for several reasons. First, one aspect of the present invention is that it is not necessary to know what device sampled the environment because it only is necessary to have the stored sample, parameters, and signature. Second, encryption is not required for authentication purposes, thereby allowing information storage devices to be manufactured in a more cost effective manner.

Other features and advantages of the present invention will become apparent from the following description.

Description of the Drawings

Fig. 1 is a schematic diagram of one embodiment of the present invention showing a digital camera, a personal computer, and an external GPS unit;

Fig. 2 is a schematic diagram of a self-contained digital camera that incorporates certain aspects of the present invention;

Fig. 2A is a detailed schematic diagram of a self-contained digital camera that incorporates certain aspects of the present invention.;

Fig. 3 is a flow chart of an operational sequence according to a first embodiment of the present invention;

Fig. 4 is a flow chart of the Pre Capture Operations from Fig. 3;

Fig. 4A1 is a flow chart of the Check Additional Inputs for Pre Capture Operations in Fig. 4;

Fig 4A2 is a continuation of the flow chart from Fig. 4A1;

Fig. 4B is a flow chart for recording the user controls during the Pre Capture Operation;

Fig. 5 is a flow chart of the Capture Operations from Fig. 3;

Fig. 6 is a flow chart of the Post Capture Operations from Fig. 3;

Fig 6B is the continuation of the flow chart from Fig. 6;

Fig. 7 is a flow chart of the Recording operation from Fig. 3;

Fig. 7A is a diagram of a file format for a signed digital image.

Fig. 8 is a flow chart of the Clean up and Preparation from Fig. 3;

Fig. 9 is a flow chart of the Authentication Sequence;

Fig. 9A1 is a flow chart of the RCA Operations from Fig. 9;

Fig. 9A2 is a continuation of the flow chart from Fig. 9A1;

Fig. 9B1 is a flow chart of the ELA/DER Operations from Fig. 9;

Fig. 9B2 is a continuation of the flow chart from Fig. 9B1;

Fig. 9B3 is a continuation of the flow chart from Fig. 9B2;

ADOBE – Exhibit 1002, page 11

JAFFE-ADOBE000045

Fig. 9B4 is a continuation of the flow chart from Fig. 9B3;

Detailed Description of the Preferred Embodiments

One aspect of the present invention is the concept and method of indigenous authentication. That is, a family of devices to create recordings with material to validate its authenticity. One embodiment of the present invention relates to digital photography where an image is authenticated as a whole. An intermediate version allows the authentication of less than the whole. An advanced version allows for recovery of damaged (altered from its original state) elements. Additional inputs including, but not limited to, date, time, latitude, longitude, altitude, roll, pitch, yaw, and compass heading can be made part of the image as well as the status of camera elements including camera identification, image sequence number, flash status, lens zoom factor, counter vibration status, focus status and focus quality. This additional information becomes part of the recording and can also be authenticated.

The present invention is applicable to information capture scenarios other than digital cameras such as self-authenticating identification documents, an extension of the notary public system, or electronic laboratory notebooks to replace the handwritten ones mentioned above. Once established as a trustworthy source; the indigenous authentication concept can be extended further for recording quality control, legal requirements and financial instruments.

A key to verifiable authenticity is to insure that the authentication information generation is tightly coupled to the sensor set and recorder. There can be nothing that can possibly alter the recording before the authentication information is generated. Authentication using this method requires neither comparison files, nor conventional or reverse encryption. The strength of authentication is increased by using one-time random elements and by the use of a random string, regenerated under user control. Although not required for basic operation, the resulting recording can be optionally encrypted to conceal the information. The absence of required conventional

encryption or reverse encryption eliminates the need for a public registrar or record keeping relating to the management of decryption keys. As the authentication is indigenous there is no requirement to identify which recorder was used.

Referring to Fig. 2, an environment 2 can be sampled 1 in a variety of formats. In recording a single sample of a visual environment, a single frame optical recorder, generally known as a camera, is used. The sample taken, known as a "photograph," has been recorded on positive transparency films (slides); negative transparency films (negatives); opaque or translucent prints; and more recently as digital files.

In recording a continuous sample of a visual environment, a continuous optical recorder such as a video camera, movie film camera or a digital movie camera is used. These samples, generically called "movies," have been recorded on transparency film, videotape and more recently as digital files.

In recording a sample of an auditory environment, a continuous audio recorder such as a tape recorder or a digital recorder is used. These samples, generally called "recordings," have been recorded on a wide variety of wire, tape and digital files.

With the development of sensors and recorders, the recording of samples of taste, touch and smell can be accommodated in the same generic model. Also, samples are not limited to the five human senses. The method for authentication and verification disclosed in the present application can be used on samples taken from any sensor set including, but not limited to, the full range of physical, chemical, and spectral phenomena.

To ensure authentication, additional inputs 7 other than the sensor set 4 are not accessible to the user without detection as shown in Fig. 2. To accomplish this the additional inputs are shown inside the device physical boundary. Analog recorders may also be incorporated into this system through the use of analog to digital converters.

One use of the present invention is to create an image or data file that is considered "trustworthy" in any situation where proof of authenticity is necessary.

ADOBE – Exhibit 1002, page 13
JAFFE-ADOBE000047

This includes, but is not limited to, legal evidence, insurance claims, project management, scientific research, invention, quality control, identification, intelligence gathering, purchasing, command and control, law enforcement, document and image transmission.

The increasingly rapid transition to digital capture, analysis, storage, transmission, distribution and use of information, using increasingly sophisticated hardware and software for creation and capture tools, makes it increasingly difficult to accept any image or data file as authentic on its face.

With the continued growth of personal computers in society and the increasing use of the internet, electronic miscreance including deliberate fraud and inadvertent changes caused by transmission or storage errors are on the rise. The need for authentication parallels that rise to counter proliferation of altered files. The need for authentication also increases with the potential damage an altered file might cause. For example, contracts, purchase orders, legal decisions, electronic bill payments, electronic invoices, quality control information, blue prints, designs: all of these could cause great harm if an altered version were believed to be authentic. It is not unreasonable to presume that indigenous authentication might become the norm, in an attempt to prevent or derail any possible malicious acts by miscreants.

One aspect of the present invention allows generally complete mitigation of the threat of undetected image alteration and subsequent use of the altered image for purposes of deliberate or unknowing deception. Thus, a framework is provided for future devices to accomplish similar ends and provide a solution to an ever more troubling social and economic problem, namely the eroding credibility of photographic images, especially in law enforcement where the images may become evidence in a legal proceeding.

Referring to Fig. 1, a schematic diagram of one embodiment of the present invention showing a digital camera, a personal computer, and an external GPS unit is shown. A general purpose microcomputer 252 is used to simulate the processor 157

ADOBE – Exhibit 1002, page 14
JAFFE-ADOBE000048

and its programming. The mouse 256 and keyboard 257 are used to simulate the user's setting of controls (See Figs. 2A, 9 10 11 12 13). The microcomputer's monitor 253 is analogous to the process monitor 8 shown in Fig. 2A. An external geographic positioning system 254 (GPS) is used instead of an internal 44 one. An externally connected digital camera 255 simulates the lens sensor set 73, auto focus 19, and flash generator 30. The microcomputer's 252 floppy drive (not shown) performs the function of the recorder 142 and the 3.5" floppy disk 259 is the removable storage media 141.

Referring to Fig. 2A, a device model for a single frame optical recorder, more commonly known as a camera, is shown. Fig. 2A does not show the externally supplied source or internal batteries that must power this device. In this camera, the user may access the process monitor 8. For approximate aiming, access may be gained through a shaft, parallel to the axis of the lens. Access to the process monitor 8 may also be gained through a processor 157 controlled recreation of the current scene. Indicators appear on the process monitor indicating flash status, zoom status, etc.

Operators may aim the device, activate the device, and set user controls, including but not limited to, flash 9, zoom 10, random string recording (RSR) 11, or optional encryption 12. During the operation of the camera, internal security 14 is monitored to detect the integrity of the tight coupling of the sensor set and the recorder 6.

Referring to Fig. 3, when the processor 157 receives an activation signal, the multi phase operating cycle proceeds through the pre capture, capture, post capture, recording, clean up and preparation operations before returning to the pre capture phase. To reduce the time within each phase, parallel processing and other engineering techniques are used.

Referring to Fig. 4, the pre capture sequence is the most common operating phase of the unit. The device cycles in the pre capture operation 65 until activated by

ADOBE – Exhibit 1002, page 15
JAFFE-ADOBE000049

user control 13, or turned off 15 in preparation for normal termination 95. If the device is turned on and inadequate 16 power is present to complete the operating cycle, the user activation will have no effect. An indication 17 is given to the user through the process monitor and no further processing is completed 66.

If sufficient power is present to complete the operating cycle, the additional inputs and components are checked. Referring to Fig. 4A1, the auto focus 19 sensor and processor are then checked 20. If a malfunction 21 is present the process monitor 8 will be updated with an error message 22 to inform the user.

Independent of the auto focus's status, processing continues checking the focus quality sensor 23, the flash generator 30, counter vibration unit (C-VIBE) 35 and the roll, pitch, yaw (RPY) unit 40. These tests are performed in order (20, 25, 29, 34, and 39) independent of resulting status. At each stage, if a malfunction is present, the process monitor is updated with an error message to inform the user (27, 32, 37 and 250).

Referring to Fig. 4A2, the status processing continues 42 with a check 43 of the global position system (GPS) unit 44. If there is a malfunction 45, the value "NO GPS" is recorded 46. If no malfunctions 47 are present, the current GPS coordinates and other GPS information are recorded 48 and the process monitor 8 is updated 49 with an error message or the current coordinates.

Independent of the GPS status, processing continues 50 with a check 51 of the internal compass 52. If a malfunction 53 is present, the value "NO COMPASS" is recorded 54. Otherwise 55 the current compass heading is recorded 56 and the process monitor 8 is updated 57 with an error message or the current heading.

Independent of the compass status, processing continues 58 with a check 59 of the internal security system 14. If there is a breach of security 60 the violation is recorded 61. Otherwise 62 the value "ImageGuard" is recorded 63 and the process monitor 8 is updated 64 with the violation or "ImageGuard"

ADOBE – Exhibit 1002, page 16
JAFFE-ADOBE000050

Referring to Fig. 4, after the additional inputs and components are checked 18, the user control modifications are recorded 67. Referring to Fig. 4B, the current setting for the flash generator 30 is checked 68 against the flash settings 9 provided by the user. If not identical 69, the setting for the flash generator 30 is set 70 to that provided by the user.

The user's zoom setting 10 is then checked 72 against the zoom setting of the lens 73. If not identical 74, the setting for zoom 73 is set 75 to that provided by the user. The current random string record (RSR) value is then checked 77 against the setting 11 provided by the user. If not identical 78, the RSR value is set 79 to that provided by the user. The two possible values are "Y" for "Yes, record a new random string with the next image" and "N" for "No, don't record a new random string with the next image."

The current encryption value is then checked 81 against the encryption value 12 provided by the user. If not identical 82, the current encryption value is set 83 to that provided by the user. The three possible values are "Y" for "Yes, produce an encrypted image only", "N" for "No, don't produce an encrypted image, produce an unencrypted image only" and "B" for "Produce both an encrypted image and an unencrypted image." During this process the process monitor 8 is updated 85 to reflect any changes made.

Referring to Fig. 4, once the user control modifications are recorded 67, processing continues 86 with a test 87 for adequate recording media. If there is inadequate recording media 88 the process monitor 8 is updated 89 with an error message and no further processing is completed 90 past this point.

After the test dealing with adequate recording media is completed 91, all pre capture operations are complete. A test 92 is made for the status of the activation control 13. If the control is not active 93, processing is cycled 65 and if active, processing continues 94 with capture operations

ADOBE – Exhibit 1002, page 17

JAFFE-ADOBE000051

Referring to Fig. 5, once the user activation control 13 is active, processing moves from pre capture operations (see Fig. 4) to capture operations. (see Fig. 5) Current values are acquired 96 from the GPS and Compass system. If the GPS is not active 45, the "NO GPS" value 46 is recorded. If the GPS is active 47, the GPS coordinates 48 are recorded as is the current date and time. If the Compass is active 55, the current heading is recorded and if not active 51, the "NO COMPASS" value 54 is acquired.

At this point, if required 97, the counter vibration unit (C-VIBE) is activated 98 to counter vibration. The roll, pitch and yaw (RPY) sensors are activated 99, and the need to prime 105 the flash unit is determined. A test is made for the user commanding the flash on or off 100. If the flash is commanded on 101 or auto flash detects 103 the requirement 104 for a flash, the flash is primed 105 and the image is captured with flash 108. Otherwise the image is captured without a flash 107.

Focus quality points are detected 109 by accessing the focus quality additional input 23. The number of focus quality points is selected, and the maximum range and minimum range are recorded. Here the camera uses either sound ranging, or another technology to measure depth of field. This procedure is required for auto focus and would detect the reproduction of a picture. This procedure also reports the number of points with differing ranges as well as the closest and farthest focus quality points from the camera. For example, "10p 1m Inf" would mean 10 points of differing depth, the nearest being one meter, the farthest is infinity.

Referring to Fig. 6, once the image has been captured (see Figure 5) processing moves to post capture operations. First the CCD (or other sensor) is polled 110 to gather the image and prepare it for recording. The GPS values for latitude, longitude, altitude, date, time, and satellites used for the positioning; that were previously acquired 96, are then appended 111 to the image. If the GPS was not functional 45 the "NO GPS" value 46 is appended 111 to the image. The AutoFocus status; number of focus quality points 109; maximum range and minimum range;

ADOBE – Exhibit 1002, page 18

JAFFE-ADOBE000052

flash value (commanded on, commanded off, auto-flash required, or auto-flash not required); counter vibration value (active 98 or not); roll, pitch and yaw (RPY) values; recorded compass heading 96; lens 73 zoom setting; camera identifier (CamID 124 set by the factory and unalterable by the user); current image sequence number 125; current random string 126; and file type (127 set by the factory and unalterable by the user) are all appended to the image. If internal security is compromised 60 a security violation 61 is appended 123 to the image. Otherwise the "ImageGuard" value is appended 123 to the image.

Referring to Fig. 6B, there are three levels of authentication and damaged element recovery. The initial level is total image authentication (TIA). At this level only the entire image is authenticated or not. The second level is row/column authentication (RCA) where each row and column of the picture elements (pixels) can be authenticated independently. Under RCA, less than the whole image can be authenticated. The third level is elemental level authentication (ELA) and damaged element recovery (DER).

Under the ELA structure, each and every single pixel can be authenticated independently. If a single pixel fails authentication (damaged) there are structures added to the image in the post capture operation which provide multiple methods of determining the original value of the damaged pixel. This is called damaged element recovery (DER). Initially the level of authentication and damaged element recovery is to be set at the factory so that no affiliated user control (9, 10, 11, 12, and 13) is shown. There can be only one level of authentication (TIA, RCA, ELA/DER) active per use. (See Figure 9 "Authentication Sequence" and more on authentication.)

If RCA is elected 128, the RCA structures and values are computed and appended 129 to the image. If ELA/DER is elected 130, the ELA/DER structures and values are computed and appended 131 to the image. The signature protocol used in this device is the commercially available MD5, but the signature protocol is not limited to the MD5. The digital signature 132, which is a function of the signature

ADOBE – Exhibit 1002, page 19

JAFFE-ADOBE000053

protocol (SP) being used and the block, is computed and made part of the file. (SIGNA=*f* (SP (Block))) The Block 144 is the digital data composed of the image and *optionally*: additional information, the camera id, the random string, the camera decryption key, and the RCA and ELA/DER structures and values.

If the user has elected 133 no encryption, or both encrypted and unencrypted, as set by the user control 12 and evidenced by the encryption value 83, then an unencrypted version of the complete image file is created 134. If the user has elected 135 encryption, or both encrypted and unencrypted, as set by the user control 12 and evidenced by the encryption value 83, then an encrypted version of the complete image file is created 136.

Referring to Fig. 7, if the user has elected 137 no encryption, or both encrypted and unencrypted, as set by the user control 12 and evidenced by the encryption value 83, then an unencrypted version of the complete image file is written 138 by the recorder 142 on the recording media 141. If the user has elected 139 encryption, or both encrypted and unencrypted, as set by the user control 12 and evidenced by the encryption value 83, then an encrypted version of the complete image file is written 140 by the recorder 142 on the recording media 141.

Referring to Fig. 2A, a 3.5" floppy drive 142 and removable 3.5" floppy diskette 141 is shown as the recorder and recording media. Other available recording options include flash RAM with removable memory modules, and storage not internal to the device via infra red, serial, Ethernet, Token Ring, parallel, universal serial bus (USB), firewire or other communication mode to either a single computer or a network of computers.

Referring to Fig. 7A, the files created by the Signa2 process are in a format generally accepted by the industry. Most specifically, the Signa2 files are not proprietary. Additional information is contained within the file, but the addition of the information is in compliance with the standards for the format.

ADOBE – Exhibit 1002, page 20

JAFFE-ADOBE000054

There are two braces in the figure. The first titled "Image" indicates the two elements that are viewable by programs compliant with generally accepted industry formats. Elements outside this brace are not viewable by programs compliant with generally accepted industry formats. The second 144 titled "Block" indicates the elements covered by the signature 145. Everything inside the "Block" is what is signed.

Elements shaded in gray 161 are optional and not required to fulfill the basic purpose of Signa2 devices. A tightly coupled image 146 and signature 145 are the minimum required elements for the Signa2 process.

The sensor set 73 acquires the image 146, which is the minimum viewable information. Additional data from the camera 147, viewable by the user, include: Global Positioning System (GPS) information 111; zoom settings; AutoFocus status; the results of the focus quality sampling; roll, pitch and yaw (RPY) values; the compass heading; flash status; File Type; CamID; Seq 120; and Security Value.

The GPS information 111 may include 48 latitude, longitude, altitude, date, time, satellites used in the determination or "NO GPS" 46 if there is a fault 45 with the system. The zoom setting 75 information includes the setting used by the lens 73 for capturing the image expressed either in millimeters with 50mm being "eye-normal", or in X where 1X is 50mm. The compass heading 117 includes information on which way the camera was pointing at the time the image was captured.

The flash status 114 information includes the commands, Commanded ON, Commanded OFF, Auto ON or Auto OFF. In the flash status, the first two refer to settings forced by the user and the latter two refer to the user allowing the camera to decide to flash or not and whether it did or not. There may be other options.

The CamId 119, or camera identification code, is set at the factory and part of each image. Examples are SHEP0001 or MOLL0454. Although not required for authentication it does provide a means of determining, at least initial ownership of the device.

ADOBE – Exhibit 1002, page 21

JAFFE-ADOBE000055

Seq 120, is the sequence number for unique image identification, automatically incremented. When used with CamId above BECK5102-98312 uniquely identifies the camera and the picture.

The two Security Values 123 are ImageGuard and NONVERIFIED. ImageGuard appears if no internal errors are detected and the security is not compromised. NONVERIFIED (or other indication of compromise) appears if security is compromised within the system.

Other segments within the File Structure include Camera ID 148; Random String 149; Camera Decryption Key 150; RCA and ELA/DER structures and values 160; and the digital signature 145. The Camera ID 148 is the unique camera identification, the same as above, but in a section of the file not viewable by the user. The Random String 149 is the current random string and is made part of the file. The Camera Decryption Key 150 is a camera specific decryption key that stays in the camera.

Referring to Fig. 8, this figure illustrates the process for clean up and preparation. In this portion of the process, functions not useful in pre capture operations (see Fig. 4) are deactivated and preparations are made for subsequent image capture. The counter vibration, and the roll, pitch, yaw are deactivated 151, 152 and the image sequence number is incremented 153.

If the "Random String Recording" has been set 79 to YES by the user control 11, the image itself and other information (Referring to Fig. 7A) are used to generate 155 a new random string that replaces the previous random string. The "Random String Recording" 79 is then reset 158 to NO and the user control 11 is set 159 to NO. Temporary resources used by the processor 157 are then deallocated 156 to prepare them for re-use.

It is important to note that the previous random string is used for the image just created. Therefore, frequent resetting of the random string will deter pattern recognition and increase security. This is discussed in the "Role of the random string

ADOBE – Exhibit 1002, page 22

JAFFE-ADOBE000056

in increasing the strength of the digital signature" below.

Referring to Fig. 9, authentication starts with a file believed to contain an image and the additional items (see Figure 7A) to make the file authenticatable as a Signa2 image. The authentication program must be easily and freely available from a secure public source. Otherwise someone seeking to deceive could provide a faux-authentication program to generate a forced-negative or forced-positive authentication.

The program starts 162 with a self diagnostic to insure that the authentication program itself has not been damaged or corrupted. This self diagnostic is repeated each time processing reaches this 162 point to guard against alterations made after the program has been loaded. Should the self diagnostic fail the program immediately ends with an error message. This self diagnostic procedure and the possibility of a failure are not shown on Figure 9.

Once the authentication program has been loaded the user is presented with an opportunity to select a file or elect program exit. If the user elects program exit the authentication program ends 163. If an encrypted file is selected 164, an attempt 165 is made to decrypt the file. This may require a decryption key obtained from the user or taken from the file 150. If a decryption error 166 occurs, an error message 167 is displayed and the program cycles back to start 162

If the file was not 168 encrypted or was decrypted without error 169, a test 170 is made to confirm that the file is in the Signa2 format. If the file is not 171 in Signa2 format, the file is not authenticatable 172 and the program cycles back to start 162

If the file is 173 in Signa2 format, the block 144 is separated 174 from the signature 145 and the signature is recalculated 175 from the original block 144. If the recalculated signature (SIG_R) matches 176 the provided signature (SIG_P), the image may be viewed 248 and is marked authenticated 249 as a valid image using total image authentication (TIA). The program then cycles back to start 162.

ADOBE – Exhibit 1002, page 23

JAFFE-ADOBE000057

If the two signatures do not match, and the authenticator program has been acquired from a trusted source and is free from alteration; then the image file has been damaged or altered. This is a *true-negative*, an image properly determined not to be authentic. With an uncompromised authenticator program, a Signa2 image file using TIA level authentication cannot generate *false-negatives*. The image and the signature are in a single file and altering the file, either intentionally or accidentally, constitutes invalidation and a proper negative authentication.

If the recalculated signature (SIG_R) does not 177 match the provided signature (SIG_P), a series of tests are made for one of three authentication levels. If only total image authentication (TIA) is available 178 then no further operations are available 179. The image is viewed 180 and marked unauthenticated 181. The program then cycles back to start 162.

Referring to Fig. 9, if row/column authentication (RCA) is 182 elected, processing continues with RCA Operations and the program cycles back to start 162. If row/column authentication (RCA) has not 183 been elected, a 184 test for elemental level authentication/damaged element recovery (ELA/DER) is made.

Referring to Fig. 9B1, if ELA/DER has 186 been elected, processing continues with ELA/DER Operations and the program cycles back to start 162. If ELA/DER has not been elected 185, there is an error condition as one of the three levels of authentication (TIA, RCA, ELA/DER) should be available. This error condition is handled by reporting no further operations are available 179. The image is viewed 180, marked unauthenticated 181 and the program cycles back to start 162.

Referring to Fig. 9, row/column authentication (RCA) is elected 182 when a file in a Signa2 format 173 has a signature failure 177. The signature used in comparison 145 is a single signature for the entire file. RCA structures and values 160 provide for a method of detecting errors, not at the whole file level, but at a level for each row and column. Checking each row and column provides two opportunities to detect an error for each pixel.

ADOBE – Exhibit 1002, page 24
JAFFE-ADOBE000058

Cyclic Redundancy Check (CRC) is the method used to describe this form of error detection. There are several varieties of CRC as well as other algorithms for error detection of this type. Although CRC is used here for description purposes, other error detection codes (or error *correction* codes such as Hamming and Reed-Soloman) may be implemented to augment or replace the CRC error detection code.

Referring to Fig. 9A1, a digital image consists of picture elements, known as pixels, arranged in a matrix of rows and columns. RCA Operations commence by stepping 187 through each row of the image testing 188 the CRC for internal integrity. Although CRCs do not contain an inherent internal integrity test, part of the RCA structures include additional values to test the CRC. If the CRC fails 189 this self test, all pixels in that row are marked as damaged, but potentially false negatives (PFN) 208.

If the CRC itself is ok 191, the entire row of pixels is used to compute 192 a new CRC for the row. This new CRC is compared to the original CRC. If they do not 193 match, all of the pixels in the row are marked as damaged 190. If the new CRC does 194 match the original CRC, all of the pixels in the row are marked 195 ok.

Referring to Fig. 9A2, RCA operations continue by stepping 196 through each column of the image and testing 197 the CRC of each column for internal integrity. If the CRC fails 198 this test, no further operations are conducted on the column of pixels. If the CRC itself is ok 200, the entire column of pixels is used to compute 201 a new CRC for the column. If the new CRC does not 202 match the original CRC, no further operations are conducted on this column. If the new CRC does 203 match the original CRC, all of the pixels in the column are marked 204 ok.

A pixel may be marked in one of six ways: Ok – ok from row CRC 195 and column CRC 204; Damaged – ok from row CRC 190 and column CRC 204; Damaged_{PFN} – ok from row CRC failure 189 208 and column CRC 204; Ok – null from row CRC 195; Damaged - null from row CRC 190; and Damaged_{PFN} – null

18

from row CRC failure 208. There is no second status because of column CRC failure 202.

The nature of the two operations (row and column) generate a matrix where some rows of pixels may be marked as damaged in the row operations and some of those pixels changed from damaged to ok by the column operations. This is because an entire row is marked damaged or ok. If a column is marked ok, the pixels that may have been marked damaged as part of a whole row were not in fact damaged and are changed to being ok. As an example, a single damaged pixel would cause a whole row to be marked as damaged in row operations. Column operations would mark every column ok except the column that had the damaged pixel. The end result is an image with a single pixel marked damaged.

Once the image has been authenticated the user selects 199 from a list of presented display options 205. The display options are: Option A - Display only the original image without any modification; Option B - Display the original image with damaged pixels forced to white; Option C - Display the original image with damaged pixels forced to black; Option D - Rock A and B; Option E - Rock A and C; Option F - Statistical Report; and Option G – End display options. "Rocking" refers to rapidly displaying two alternating images.

The statistical report under Option F contains the following elements: F1 contains the total number of pixels in the image. F2 contains the total number of pixels marked ok - ok, Damaged - ok, $Damaged_{PFN}$ - ok and ok - null, expressed as a number, and as a relative percent of the total number of pixels (F2/F1)*100 known as the "Undamaged Percentage."

Ok - ok pixels passed both row 194 and column 203 CRC test. Ok - null pixels passed the row 194 CRC test, but the column CRC was damaged 198 and provided no additional information. Damaged - ok pixels were not actually damaged. The pixels were marked damaged because the new row CRC did not match 193 the original row CRC, and the whole row was marked 190 damaged even though the

ADOBE – Exhibit 1002, page 26
JAFFE-ADOBE000060

pixels passed 203 the column CRC test. $Damaged_{PFN}$ - ok also contains pixels that were not actually damaged. The pixels were marked damaged due to the row CRC failure 189 that caused the entire row to be marked $Damaged_{PFN}$ even though the pixels passed 203 the column CRC test.

F3 contains the total number of pixels marked Damaged - null expressed as a number, and as a relative percent of the total number of pixels in the image (F3 / F1) * 100 known as the "True Negative Percentage." The pixels were marked Damaged - null because the new row CRC did not match the original row CRC test 193. There is no second status because of column CRC failure 202.

F4 contains the total number of pixels marked $Damaged_{PFN}$ - null expressed as a number, and as a relative percent of the total number of pixels in the image (F4 / F1) * 100 known as the "Potential False Negative Percentage." The pixels were marked $Damaged_{PFN}$ - null because the row CRC failed 189 208 the self test and the pixel could not be authenticated as ok due to column CRC failure 202. The sum of the relative percents of F2, F3, and F4 should equal 100%, and the sum of F2, F3, and F4 should equal F1.

The user may continue to select 206 alternate display options until they elect to end display options 207. At that point RCA operations are concluded.

Referring to Fig. 9B1, ELA/DER Operations occur when a file in Signa2 format 173 has a signature failure 177, and both element level authentication (ELA) and damaged element recovery (DER) authentication are elected 186. The signature used in comparison 145 is a single signature for the entire file. ELA/DER structures and values 160 provide for a method of determining authentication, not at the whole file level, but at a level for each element.

The ELA/DER structure includes a complete duplicate of the image, compressed and encoded. It is this duplicate image that allows for elemental level authentication and damaged element recovery. In the description below the original version of the image, the one the user can see, is referred to as the "Primary Image",

abbreviated PI. The compressed and encoded version of the image is referred to as the "Backup Image", abbreviated BI. Both the Primary Image and the Backup Image have row and column CRCs, or other error detection protocols.

Referring to Fig. 9B1, initially each row 209 of the primary image (PI) is stepped through and a self test 210 is performed on each primary image row CRC. If the CRC fails 211 the self test, all of the pixels in the primary image row are marked 212 $Damaged_{PFN}$ as potential false negative damaged pixels. If the primary image row CRC passes 213 the self test, a new primary row CRC is computed 214 from the pixels in the primary image row. If the new primary image row CRC matches 215 the original primary row CRC, all the pixels in the row are marked 216 as ok (undamaged). If the new primary image row CRC does not 217 match the original primary row CRC, all the pixels in the row are marked 218 as damaged.

Referring to Fig. 9B2, once the row-wise process is complete, each column 219 of the primary image is stepped through with a self test 220 performed on the primary image column CRC. If the CRC fails the self test 221, no further operations are conducted on this column. If the primary image column CRC passes 222 the self test, a new primary column CRC is computed 223 from the pixels in the primary image column. If the new primary image column CRC matches 225 the original primary image column CRC, all of the pixels in that column are marked 226 ok. If the new primary image column CRC does not 224 match the original primary image column CRC, no further operations are conducted on this column.

Each pixel may be marked in one of six ways: Ok – ok from row CRC 216 and column CRC 226; Damaged – ok from row CRC 218 and column CRC 226; $Damaged_{PFN}$ – ok from row CRC failure 212 and column CRC 226; Ok – null from row CRC 216; Damaged – null from row CRC 218; and $Damaged_{PFN}$ – null from row CRC failure 212. There is no second status because of column CRC failure 221

Referring to Fig. 9B3, authentication then starts on each damaged or $damaged_{PFN}$ pixel with attempts to recover the original value of that element.

ADOBE – Exhibit 1002, page 28

JAFFE-ADOBE000062

Additional processing efforts are not made to distinguish between true negatives and false negatives due to the fact that the same damaged element recovery (DER) procedures are used on each.

To recover the value of a damaged primary image pixel the corresponding backup image pixel must first be located and validated. Validation of the corresponding backup image pixel can occur under *either* of the two scenarios. In the first scenario, the backup image ROW CRC for the corresponding backup image pixel is undamaged and the computed backup image ROW CRC matches the original backup image ROW CRC. In the second scenario, the backup image COLUMN CRC for the corresponding backup image pixel is undamaged and the computed backup image COLUMN CRC matches the original backup image COLUMN CRC.

Stepping 227 through each damaged or damaged$_{PFN}$ pixel in the primary image is done to locate 228 the corresponding pixel in the backup image. The backup image will require decompression first. If the corresponding backup image pixel cannot 229 be located, it cannot be authenticated and it is not possible to recover the value of the primary image pixel 230. Once the corresponding backup image pixel is 231 located, a self test 232 is performed on the backup image ROW CRC.

If the backup image ROW CRC self test fails 233, the backup image ROW CRC is damaged and is unusable for authentication. The backup image COLUMN CRC for the corresponding backup image pixel is then used for authentication and a self test 235 of the backup image COLUMN CRC is performed.

If the backup image COLUMN CRC for the corresponding backup image pixel fails 236 the self test, the corresponding backup image pixel cannot be authenticated and it is not possible to recover the value of the primary image pixel 230. If the backup image COLUMN CRC for the corresponding backup image pixel passes 239 the self test then a new backup image COLUMN CRC is computed 240.

If the new backup image COLUMN CRC matches 241 the original backup image COLUMN CRC 238, the corresponding backup image pixel is authentic and

can be used to recover the value of the damaged or damaged$_{PFN}$ primary image pixel. If the new backup image COLUMN CRC does not match 243 the original backup image COLUMN CRC, the corresponding backup image pixel cannot be authenticated and it is not possible to recover the value of the primary image pixel 230.

If the backup image ROW CRC self test succeeds 234, a new backup image ROW CRC is computed 251. If the new backup image ROW CRC matches 237 the original backup image ROW CRC then 238 the corresponding backup image pixel is authentic and can be used to recover the value of the damaged or damaged$_{PFN}$ primary image pixel. If the new backup image ROW CRC does not 242 match the original backup image ROW CRC, one or more of the backup image pixels in that row is damaged and the backup image column must be tested for authentication.

A self test 235 of the backup image COLUMN CRC is performed. If the backup image COLUMN CRC for the corresponding backup image pixel fails 236 the self test, the corresponding backup image pixel cannot be authenticated and it is not possible to recover the value of the primary image pixel 230. If the backup image COLUMN CRC for the corresponding backup image pixel passes 239 the self test then a new backup image COLUMN CRC is computed 240.

If the new backup image COLUMN CRC matches 241 the original backup image COLUMN CRC 238, the corresponding backup image pixel is authentic and can be used to recover the value of the damaged or damaged$_{PFN}$ primary image pixel. If the new backup image COLUMN CRC does not match 243 the original backup image COLUMN CRC then the corresponding backup image pixel cannot be authenticated and it is not possible to recover the value of the primary image pixel 230.

Each pixel may then be marked in one of eight ways: Ok – ok, from row CRC 216 and column CRC 226; Damaged – ok, from row CRC 218 and column CRC 226; Damaged$_{PFN}$ – ok, from row CRC failure 212 and column CRC 226; Ok – null, from

ADOBE – Exhibit 1002, page 30
JAFFE-ADOBE000064

row CRC 216; Damaged - null – recovered, from row CRC 218 (The original value of the pixel was recovered 238); Damaged - null - not recovered, from row CRC 218 (the original value of the pixel was not 230 recovered); Damaged$_{PFN}$ - null – recovered, from row CRC failure 212 (the original value of the pixel was recovered 238); and Damaged$_{PFN}$ - null - not recovered, from row CRC failure 212 (the original value of the pixel was not 230 recovered). Damaged - null and Damaged$_{PFN}$ - null are replaced with the results of the recovery efforts

Referring to Fig. 9B4, once the authentication and recovery operations are completed the user is presented 244 with a list of eleven presented display options 245. Option A display only the original image without any modification Option B display the original image with damaged and damaged$_{PFN}$ pixels forced to white. Option C display the original image with damaged and damaged$_{PFN}$ pixels forced to black. Option D display the original image with damaged and damaged$_{PFN}$ pixels replaced with recovered pixels. Unrecovered damaged and damaged$_{PFN}$ pixels are forced to white. Option E display the original image with damaged and damaged$_{PFN}$ pixels replaced with recovered pixels. Unrecovered damaged and damaged$_{PFN}$ pixels are forced to black.

Rapidly displaying two alternating images is known as "rocking." Option F rocks between A and B. Option G rocks between A and C. Option H rocks between A and D. Option I rocks between A and E.

Option J displays the Statistical Report containing the various elements. This option displays the total number of pixels in the image J1. It also displays the total number of pixels marked ok - ok, Damaged - ok, Damaged$_{PFN}$ - ok and ok - null, expressed as a number, and as a relative percent of the total number of pixels (J2/J1)*100 known as the "Undamaged Percentage" J2. Ok - ok pixels are those that passed both row 216 and column 226 CRC test. Ok - null pixels are those that passed the row 216 CRC test, but the column CRC was damaged 221 and provided no additional information. Damaged - ok pixels are those that were not actually

damaged. The pixels were marked damaged because the new row CRC did not match 217 the original row CRC and the whole row was marked 218 damaged. These pixels passed 225 the column CRC test. Damaged$_{PFN}$ - ok pixels were those that were not actually damaged. The pixels were marked damaged$_{PFN}$ because of row CRC failure 211 caused the entire row to be marked 212 Damaged$_{PFN}$. The pixels passed 225 the column CRC test.

Option J also displays the total number of damaged - null – recovered pixels as a number, and as a relative percent of the total number of pixels (J3/J1)*100 known as the "Damaged and Recovered Pecentage" J3. The total number of damaged - null - not recovered pixels are also displayed as a number and as a relative percent of the total number of pixels (J4/J1)*100 known as the "Damaged and Not Recovered Pecentage" J4.

Option J displays the total number of damaged$_{PFN}$ - null - recovered pixels as a number and as a relative percent of the total number of pixels (J5/J1)*100 known as the "Damaged$_{PFN}$ and Recovered Pecentage" J5. It also displays the total number of damaged$_{PFN}$ - null - not recovered pixels as a number and as a relative percent of the total number of pixels (J6/J1)*100 known as the "Damaged$_{PFN}$ and Not Recovered Pecentage" J6. The sum of J2, J3, J4, J5 and J6 should equal J1, and the sum of the relative percents of J2, J3, J4, J5 and J6 should equal 100%.

The final option that may be selected is Option K to end display options. The user may continue to select 246 alternate display options until they elect to end display options 247. At that point ELA/DER operations are concluded.

The following is information on True Negatives, False Negatives and False Positives using row/column authentication (RCA) given that an authenticator program has been acquired from a trusted source and is free from alteration.

If a pixel is damaged (altered from its original state) and this damage is detected by the RCA operations then the pixel is a true-negative, part of an image properly determined not to be authentic. Using RCA it is possible to generate a false

negative, that is where a pixel is in fact authentic, but is being marked as damaged.

There are eight possible cases of pixel authenticity / damage, row CRC authenticity / damage, and column CRC authenticity / damage.

Case	A	B	C	D	E	F	G	H
Pixel Damaged	N	Y	N	N	Y	Y	N	Y
Row CRC Damaged	N	N	Y	N	Y	N	Y	Y
Col CRC Damaged	N	N	N	Y	N	Y	Y	Y

Y = damaged N = not damaged or ok

The number of possibilities can be expressed as

$$\frac{\text{(The number of elements) !}}{\text{(Number of identical elements) !}}$$

There are three elements in all cases. Case A is the case in which none of the three items are damaged. There is the single case with zero Y and three N. (3!/3!=1) Cases B through D are the cases in which a single item of the three are damaged. There are three cases with one Y and two N. (3!/2!=3.) Cases E through G are the cases in which two of the three items are damaged. There are three cases with two Y and one N. (3!/2!=3.) Case H is the case in which three of the three items are damaged. There is one case with three Y and zero N. (3!/3!=1.)

Only in case G where both the row CRC and column CRC are damaged, and the pixel is not damaged, would a false negative be generated. Failure 189 of the row CRC self test would cause all the pixels in the row to be marked damaged$_{PFN}$ 190. The column CRC would also fail 198 the column CRC self test and the pixel would remain marked as damaged$_{PFN}$. In case H, both the row CRC and column CRC are damaged and would appear to mimic case G, except that this is not a false negative because the pixel is also damaged.

Using the same table it can be shown that a false positive (a damaged pixel

ADOBE – Exhibit 1002, page 33
JAFFE-ADOBE000067

being improperly authenticated as undamaged) is not a possible condition. Cases B, E, F, and H have damaged pixels. In case B, the row CRC is undamaged and the newly computed 192 row CRC would not 193 match the original row CRC. Thus all pixels in the row would be marked 190 as damaged. In case B the column CRC is also undamaged. The computed new column CRC 201 would not 202 match the original CRC and the pixels in the column marked as damaged would remain marked as damaged. Only if the new column CRC matches the original column CRC 203 would all the pixels in the column, including the damaged one, be marked 204 as ok.

In case E, the row CRC is damaged and it would fail 189 the row CRC self test 188 causing all pixels in the row to be marked 208 as $damaged_{PFN}$. The column CRC is undamaged and would pass 200 the column CRC self test. The new column CRC would not 202 match the original CRC and the pixels in the column marked as $damaged_{PFN}$ would remain marked as damaged due to the fact that when a row CRC is damaged, the row of pixels is marked as "damaged potential false negative" or $damaged_{PFN}$. Only if the new column CRC matches the original column CRC 203 would all the pixels in the column, including the damaged one, be marked 204 as ok.

In case F, the row CRC is undamaged and would pass 191 the row CRC self test 188. The newly computed row CRC 192 would not match 193 the original row CRC causing all of the pixels in the row to be marked 190 damaged. In case F, the column CRC is damaged and it would not 198 pass the CRC self test and the pixels in the column marked as damaged would remain marked as damaged.

In case H, the row CRC is damaged and would fail 189 the row CRC self test 188 causing all pixels in the row to be marked 208 as $damaged_{PFN}$. In case H, the column CRC is damaged and would not 198 pass the CRC self test. The pixels in the column marked as $damaged_{PFN}$ would remain marked as $damaged_{PFN}$ due to the fact that when a row CRC is damaged, the row of pixels is marked as "damaged potential false negative" or $damaged_{PFN}$.

Under RCA, false positives, a damaged pixel being improperly authenticated as undamaged, cannot occur if the authenticator program has been acquired from a trusted source and is free from alteration

The following is information on True Negatives, False Negatives and False Positives using element level authentication (ELA) with damaged element recovery (DER). If a pixel is damaged (altered from its original state) and the damage is detected by the ELA operations then the pixel is a true-negative, part of an image properly determined not to be authentic. Using ELA it is possible to generate a false-negative, that is where a pixel is in fact authentic, but is being marked as damaged.

There are sixty-four (64) possible cases of primary image pixel authenticity / damage, backup image pixel authenticity / damage, primary row CRC authenticity / damage, backup row CRC authenticity / damage, primary column authenticity / damage, and backup column CRC authenticity / damage.

In table form these cases are

Y = damaged N = not damaged or ok

Group 1 Primary Image pixel is authentic and Backup Image pixel is authentic

Case	A1	B1	C1	D1	E1	F1	G1	H1	I1	J1	K1	L1	M1	N1	O1	P1
Primary Image Pixel	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Backup Image Pixel	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Primary-Row CRC	N	Y	N	N	N	Y	Y	Y	N	N	N	Y	Y	Y	N	Y
Backup-Row CRC	N	N	Y	N	N	Y	N	N	Y	Y	N	Y	Y	N	Y	Y
Primary-Column CRC	N	N	N	Y	N	N	Y	N	Y	N	Y	Y	N	Y	Y	Y
Backup-Column CRC	N	N	N	N	Y	N	N	Y	N	Y	Y	N	Y	Y	Y	Y

Group 2 Primary Image pixel is damaged and Backup Image pixel is authentic

Case	A2	B2	C2	D2	E2	F2	G2	H2	I2	J2	K2	L2	M2	N2	O2	P2
Primary Image Pixel	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Backup Image Pixel	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Primary-Row CRC	N	Y	N	N	N	Y	Y	Y	N	N	N	Y	Y	Y	N	Y
Backup-Row CRC	N	N	Y	N	N	Y	N	N	Y	Y	N	Y	Y	N	Y	Y
Primary-Column CRC	N	N	N	Y	N	N	Y	N	Y	N	Y	Y	N	Y	Y	Y
Backup-Column CRC	N	N	N	N	Y	N	N	Y	N	Y	Y	N	Y	Y	Y	Y

Group 3 Primary Image pixel is authentic and Backup Image pixel is damaged

Case	A3	B3	C3	D3	E3	F3	G3	H3	I3	J3	K3	L3	M3	N3	O3	P3
Primary Image Pixel	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Backup Image Pixel	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Primary-Row CRC	N	Y	N	N	N	Y	Y	Y	N	N	N	Y	Y	Y	N	Y
Backup-Row CRC	N	N	Y	N	N	Y	N	N	Y	Y	N	Y	Y	N	Y	Y
Primary-Column CRC	N	N	N	Y	N	N	Y	N	Y	N	Y	Y	N	Y	Y	Y
Backup-Column CRC	N	N	N	N	Y	N	N	Y	N	Y	Y	N	Y	Y	Y	Y

Group 4 Primary Image pixel is damaged and Backup Image pixel is damaged

Case	A4	B4	C4	D4	E4	F4	G4	H4	I4	J4	K4	L4	M4	N4	O4	P4
Primary Image Pixel	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Backup Image Pixel	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

ADOBE – Exhibit 1002, page 36

JAFFE-ADOBE000070

Primary-Row CRC	N	Y	N	N	N	Y	Y	Y	N	N	N	Y	Y	Y	N	Y
Backup-Row CRC	N	N	Y	N	N	Y	N	N	Y	Y	N	Y	Y	N	Y	Y
Primary-Column CRC	N	N	N	Y	N	N	Y	N	Y	N	Y	Y	N	Y	Y	Y
Backup-Column CRC	N	N	N	N	Y	N	N	Y	N	Y	Y	N	Y	Y	Y	Y

In order to be a false negative: (1) the primary image pixel must be, in fact, undamaged (N); (2) initial operations must improperly indicate that the primary image pixel is damaged; and (3) all subsequent operations must fail to correct that improper indication.

The factor that in a false negative the primary image pixel must be, in fact, undamaged (N) limits the results to Group 1 and Group 3. The primary row CRC must be damaged (Y) to initially mark a row of PI pixels as damaged$_{PFN}$. If the ROW CRC is undamaged and the row of pixels is undamaged, then pixel will be marked ok. This is not a negative, false or otherwise and limits the results to cases B, F, G, H, L, M, N and P in Group 1 and Group 3.

The primary column CRC must be damaged (Y) to preclude the correction of a pixel marked damaged by a damaged row CRC. In cases B, F, H, and M, the primary column CRC is undamaged (N) which would correct the improper identification of the pixel as damaged$_{PFN}$ limiting the results to cases G, L, N and P in Group 1 and Group 3.

The backup row CRC must be damaged (Y) to preclude correction. In cases G and N, the backup row CRC is undamaged (N) and would correct the improper identification of the pixel as damaged limiting the results to case L and P in Group 1 and Group 3.

The backup column CRC must be damaged (Y) to preclude correction. In case L, the backup column CRC is not damaged (N) and would correct the improper identification of the pixel as damaged$_{PFN}$. In case P1, the backup image pixel is also

ADOBE – Exhibit 1002, page 37

JAFFE-ADOBE000071

authentic, but because of the damage to all of the error detection structures (primary row CRC, primary column CRC, backup row CRC and backup column CRC) it cannot be validated as authentic. Only in cases P1 and P3 could an authentic pixel be marked damaged without the possibility of correction.

Using the same tables it can be shown that a false positive (a damaged pixel being improperly authenticated as undamaged) is not a possible condition. Group 2 and Group 4 both contain damaged primary image pixels. If the primary row CRC is damaged, all pixels in the row are marked damaged. If the primary row CRC is undamaged, the new row CRC will not match the provided row CRC and all pixels in the row will be marked damaged. For the purposes of isolating a case of false positive, it does not matter if the primary row CRC is damaged (Y) or not (N). The pixel will be marked as damaged or damaged$_{PFN}$. Again, the primary image ROW CRC alone guarantees that a damaged pixel will be marked damaged or damaged$_{PFN}$.

To be a false positive all detective and corrective mechanisms must fail in a mode to change the primary row CRC determination that the pixel is damaged or damaged$_{PFN}$. If the primary column CRC is damaged 221 it will not change the determination that a pixel is damaged. If the primary column CRC is undamaged 222 the new PI COLUMN CRC will not match the original PI COLUMN CRC. Thus, it will not change the determination that a damaged pixel is damaged. For the purposes of isolating a case of false positive it does not matter if the primary column CRC is damaged (Y) or not (N). The damaged pixel will remain marked as damaged.

Backup row and column CRCs are used for damaged element recovery, not element level authentication. Thus, for the purposes of isolating a case of false positive it does not matter if the backup row CRC is damaged (Y) or not (N), and it does not matter if the backup column CRC is damaged (Y) or not (N). The damaged pixel will remain marked as damaged.

This eliminates all cases in Group 2 and Group 4 as possible sources of a false positive condition. As no other cases remain for consideration, false positives are not

ADOBE – Exhibit 1002, page 38

JAFFE-ADOBE000072

possible if the authentication program is free from unauthorized alteration.

Using the same tables we can determine if a damaged pixel can or cannot be recovered from the damaged element recovery structures. To be considered for recovery a primary image pixel must be either, in fact damaged or a false-negative (a pixel marked damaged that is, in fact, undamaged). This limits consideration to damaged pixels in Groups 2 and 4, and cases P1 and P3 for the two possible false-negative situations.

The backup image pixel must be, in fact, undamaged. All Group 4 cases where the BI pixel is damaged are not recoverable due to the fact that all false positives are not possible. The backup image control structures must authenticate it the BI pixel as undamaged. The backup row CRC can be damaged which would lead to the backup image pixel being improperly considered damaged. If the backup column CRC were undamaged, it would correct the improper designation of the backup image pixel as damaged.

An undamaged backup row CRC would indicate that the backup image pixel is undamaged. A damaged backup column CRC would not change the determination of the backup row CRC that the backup image pixel is undamaged. Thus, as long as either the backup image row CRC or backup image column CRC are undamaged, an undamaged backup image pixel can be authenticated and used to recover the damaged primary image pixel. Only in cases J2, M2, O2 and P2 are both the backup image CRC structures damaged and unable to authenticate the undamaged backup image as undamaged.

In the false positive cases of P1 and P3, both of the backup CRC structures are damaged and unable to authenticate the undamaged backup image as undamaged. Therefore, in all 16 cases of Group 4, cases J2, M2, O2 and P2, a damaged primary image pixel cannot be recovered. If P1 or P3 generates a false negative, the improperly identified damaged primary image pixel cannot be recovered.

ADOBE – Exhibit 1002, page 39

JAFFE-ADOBE000073

The following is information on the role of the random string in increasing the strength of the digital signature. A series of examples and explanations shows how the use of one time and random elements increase the resistance of a digital signature to successful fraudulent impersonation.

Starting with a blank image and a constant signature algorithm, any true image could be altered to blank and the signature from a truly blank image could be added. The resulting altered image would be improperly validated as authentic with little effort. Clearly this is a weaker situation and an undesirable outcome as the same image generates the same signature.

In the adaptive signature, a signature is generated from the contents of the image. In the case of a blank image, the same signature would be generated. An image could be manipulated to blank and the signature duplicated from a properly signed blank image. This would allow the improper validation as authentic in a manner similar to the preceding with the same undesirable outcome.

An example of an adaptive signature is one that contains a one-time element. The addition of a one-time element allows for differing signatures even if the image itself is blank. One-time elements are never repeated such as date-time or image sequence number. Some convolution or manipulation of these one-time elements is desirable to preclude their easy forgery. This is a stronger solution as the same image generates differing signatures.

An adaptive signature may also be a signature that contains one-time elements and random elements. A "random string" is a sequence of characters generated from many variables including selected values from a previous image. The algorithm to create the random string is a trade secret and may differ from device to device even among the same production run of otherwise identical devices. The algorithm used may also vary from use to use of the same device. Two blank images captured a second apart with the same device can generate two widely different signatures. Two blank images captured at the exact same moment by two different devices can

ADOBE – Exhibit 1002, page 40
JAFFE-ADOBE000074

generate two widely different signatures. This creates a stronger solution than the adaptive signature containing only a one-time element.

Another variation is an adaptive signature with a one-time element and a one-time random element. The user has control over how often a new random string is created. If the random string were created anew after each image was captured, then pattern recognition of the resulting signature from the image is not possible as random elements are, by definition, not patterned. Unless the signature generation protocol and the random string generation algorithm were known or reverse engineered, the ability to sign a properly constituted Signa2 image resides solely inside the Signa2 devices. By varying the random string generation protocol between devices, varying between protocols between use to use of the same device, and regenerating the random string frequently, analysis of the results to determine the process (a form of reverse engineering) is an almost fruitless exercise.

While the invention has been illustrated and described in detail in the drawings and foregoing description, the same is considered as illustrative and not restrictive in character, it being understood that all changes and modification that come within the spirit of the invention are desired to be protected.

ADOBE – Exhibit 1002, page 41
JAFFE-ADOBE000075

What is claimed is

1. An apparatus for allowing a data stream to be authenticated, comprising:

a memory; and

a circuit that is adapted to store a data stream in said memory, said circuit allowing it to be determined whether or not the data stream has been altered after it has been stored in said memory by:

storing at least one parameter in said memory with said data string, said at least one parameter being generally representative of at least one condition under which said data stream was generated,

utilizing said data stream and said at least one parameter to generate a first signature that is stored in said memory with said data stream,

generating a second signature from said data stream and said stored at least one parameter, and

determining whether said first and second signatures are the same.

2. The apparatus of claim 1 wherein said circuit and said memory form a part of a digital camera.

3. The apparatus of claim 1 wherein said at least one parameter is selected from a group consisting of: a random number, GPS coordinates, zoom settings, AutoFocus status, focus quality sampling, roll, pitch and yaw values, compass headings, flash status, CamID, Seq, and a Security Value.

4. The apparatus of claim 1 wherein said data stream is a digital sample of an environment.

5. A method for allowing a data stream to be authenticated comprising the steps of:

storing a data stream in a memory;

35

storing at least one parameter in said memory, said at least one parameter being generally representative of at least one condition under which said data stream was generated;

utilizing said data stream and said at least one parameter to generate a first signature that is stored in said memory with said data stream;

generating a second signature from said data stream and parameters at a point in time subsequent to computation of said first signature; and

comparing said first and second signature to see whether said first and second signatures are the same.

6. The method of claim 5 wherein said circuit and said memory form a part of a digital camera.

7. The method of claim 5 wherein said data stream is a digital sample of an environment.

8. The method of claim 5 wherein said at least one parameter is selected from a group consisting of: a random number, GPS coordinates, zoom settings, AutoFocus status, focus quality sampling, roll, pitch and yaw values, compass headings, flash status, CamID, Seq, and a Security Value.

Abstract of the Disclosure

A method and system of authentication for sensor-recorders and other information capture devices is disclosed. In accordance with aspects of the current invention, a digital sample of the environment is obtained. From this sample and at least one parameter representative of at least one condition under which the sample was generated, a digital signature is created. This signature is stored in memory with the sample to be checked at a later time for authenticity. The file is checked for authenticity by generating a second signature from the file and comparing that signature to the original signature. If the two signatures are identical, the sample is considered authentic and if the two signatures are different, the sample cannot be authenticated.

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare:

That my residence, post office address and citizenship are as stated below next to my name.

That I verily believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural inventors are named below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**

the specification of which (check one)
(X) is attached hereto.
( ) was filed on _____ as
Application Serial No._____
and was amended on _____
(if applicable)

That I have reviewed and understand the contents of the above-identified specification, including the claim, as amended by any amendment referred to above.

That I acknowledge the duty to disclose information known to be material to patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

That I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate on this invention having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐ Yes ☐ No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐ Yes ☐ No

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below.

_____ (Application Number) _____ (Filing Date)

_____ (Application Number) _____ (Filing Date)

That I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

United States Application(s)

_____ (Application Serial No.)	_____ (Filing Date)	_____ (Status)-(Patented, pending, abandoned)
_____ (Application Serial No.)	_____ (Filing Date)	_____ (Status)-(Patented, pending, abandoned)

That all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

I hereby appoint the following attorneys, with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith and request that all correspondence and telephone calls in respect to this application be directed to WELSH & KATZ, LTD., 120 South Riverside Plaza, 22nd Floor, Chicago, Illinois 60606, Telephone No. (312) 655-1500:

Attorney	Registration No.
A. Sidney Katz	24,003
Richard L. Wood	22,869
Jerold B. Schnayer	28,903
Eric C. Cohen	27,429
Joseph R. Marcus	25,060
Gerald S. Schur	22,053
Gerald T. Sheklelon	27,466
James A. Schear	29,434
Daniel R. Cherry	29,054
Edward P. Gamson	29,381
Kathleen A. Rhaligan	34,044
Thomas W. Tolpin	27,600
Jon P. Christensen	34,137
Eric D. Cohen	38,110
Walter J. Kawula, Jr.	39,724
Philip D. Segrest, Jr.	39,021
Mitchell J. Weinstein	37,963
Jeffrey W. Salmon	37,435

Full name of sole or one joint inventor: Jonathan E. Jaffe

Inventor's signature:

Date: 7/27/2000

Residence and Post Office Address: 6603 Bradfield Blvd
Gurnee, IL 60031

Citizenship: USA

Full name of sole or one joint inventor: Joel D. Goldhar

Inventor's signature:

Date: 7/27/2000

Residence and Post Office Address: 720 Foxdale Ave.
Winnetka, IL 60093

Citizenship: USA

TOTAL P.02

JUL-27-00 THU 13:21 Hazel Corporation P.02

That all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

I hereby appoint the following attorneys, with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith and request that all correspondence and telephone calls in respect to this application be directed to WELSH & KATZ, LTD., 120 South Riverside Plaza, 22nd Floor, Chicago, Illinois 60606, Telephone No. (312) 655-1500:

Attorney	Registration No.
A. Sidney Katz	24,003
Richard L. Wood	22,839
Jerold B. Schnayer	28,903
Eric C. Cohen	27,429
Joseph R. Marcus	25,060
Gerald S. Schur	22,053
Gerald T. Shekleton	27,466
James A. Scheer	29,434
Daniel R. Cherry	29,054
Edward P. Gamson	29,381
Kathleen A. Rheintgen	34,044
Thomas W. Tolpin	27,600
Jon P. Christensen	34,137
Eric D. Cohen	38,110
Walter J. Kawula, Jr.	39,724
Philip D. Segrest, Jr.	39,021
Mitchell J. Weinstein	37,963
Jeffrey W. Salmon	37,435

Full name of sole or one joint inventor: Jonathan E. Jaffe

Inventor's signature: _____

Date: _____

Residence and Post Office Address: _____

_____

Citizenship: _____

Full name of sole or one joint inventor: Joel D. Goldhar

Inventor's signature: Joel D. Goldhar

Date: 7/27/2000

Residence and Post Office Address: 720 Foxdale Av.
Winnetka, IL. 60093

Citizenship: USA

Full name of sole or one joint inventor:	Michael A. Warot
Inventor's signature:	Michael A Warot
Date:	July 27, 2000
Residence and Post Office Address:	532 Florence Hammond, Indiana, 46324
Citizenship:	United States

Address for Correspondence:

WELSH & KATZ, LTD.
120 South Riverside Plaza
22nd Floor
Chicago, Illinois 60606

09625548.030600

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of	)	
	)	
JONATHAN E. JAFFE ET AL.	)	
	)	
Serial No.	)	
	)	Examiner:
Filed:	)	
	)	Group Art Unit:
For: INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES	)	Docket No. 6468/78445

ASSOCIATE POWER OF ATTORNEY

Assistant Commissioner
for Patents
Washington, D.C. 20231

Sir:

As attorney of record for applicants Jonathan E. Jaffe et al., I hereby appoint Daniel M. Gurfinkel, Registration No. 34,177, of Welsh & Katz, Ltd., 120 South Riverside Plaza, 22nd Floor, Chicago, Illinois 60606, as associate attorney with full power to transact business on behalf of applicants, Jonathan E. Jaffe et al., in connection with the above application.

Respectfully submitted,

Gerald T. Shekleton

Gerald T. Shekleton
Registration No. 27,466

Applicant or Patentee: Jonathan E. Ja ɔel D. Goldhar and Michael A. Warot y Docket No. 6468/78445
Serial or Patent No.: Not yet assigne.
Filed or Issued: Herewith
For: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS
(37 CFR 1.9(f) AND 1.27(c) - SMALL BUSINESS CONCERN)

I hereby declare that I am

( ) the owner of the small business concern identified below:
(X) an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN: Goldhar/Jaffe Technology Development Corporation
ADDRESS OF CONCERN: 720 Foxdale Av., Winnetka, IL. 60093

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.12, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time, or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, entitled:

INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES

by inventor(s): Jonathan E. Jaffe, Joel D. Goldhar and Michael A. Warot
described in:

(X) the specification filed herewith.
( ) application serial no. _____, filed _____.
( ) Patent No. _____, issued _____.

If the rights held by the above-identified small business concern are not exclusive, each individual, concern, or organization having rights to the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e). *NOTE: Separate verified statements are required from each named person, concern, or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

NAME _____
ADDRESS _____
( ) INDIVIDUAL ( ) SMALL BUSINESS CONCERN ( ) NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING: Joel D. Goldhar
TITLE OF PERSON OTHER THAN OWNER: President
ADDRESS OF PERSON SIGNING: 720 Foxdale Av., Winnetka, IL. 60093
SIGNATURE: Joel D. Goldhar Date: 7/27/2000

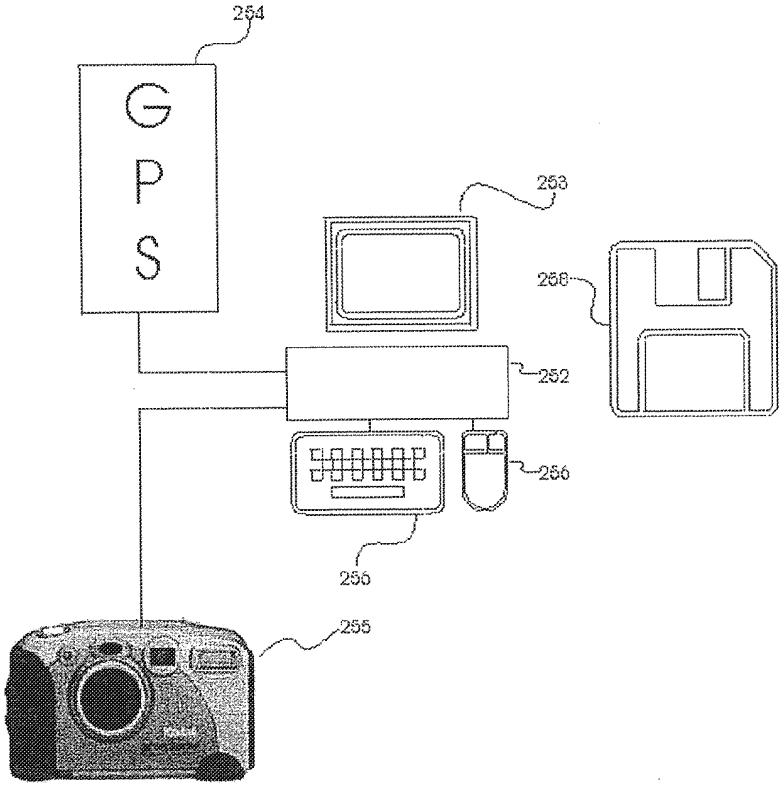


FIGURE 1

17

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 1 of 21

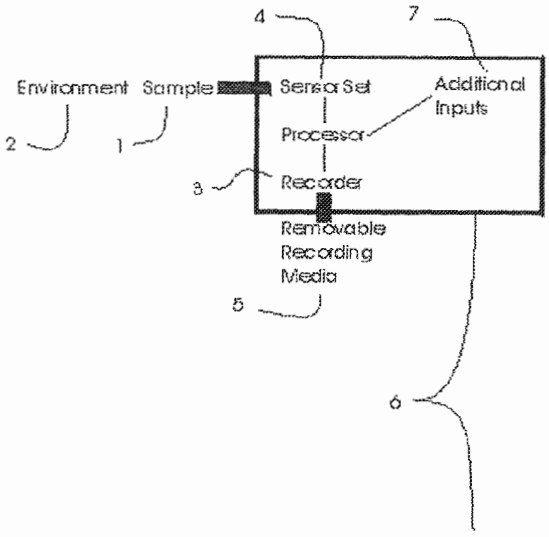
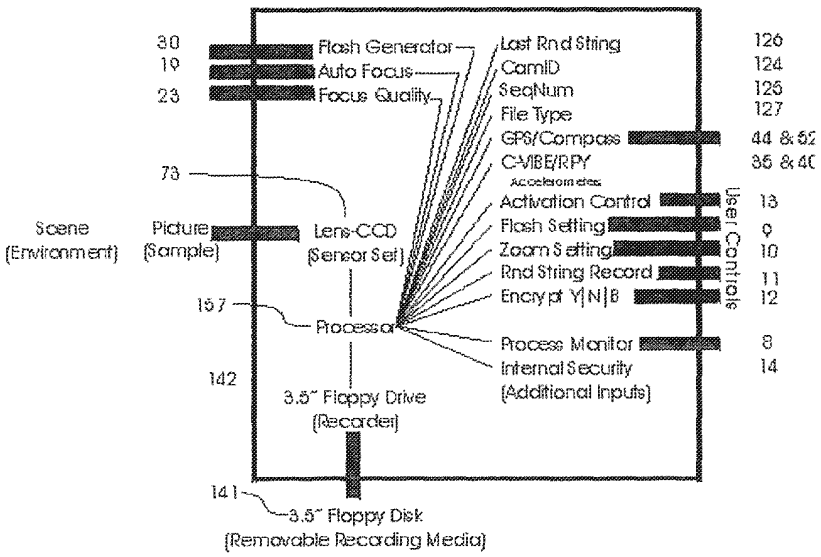

4
7
Environment
Sample
Sensor Set
Additional Inputs
2
1
Processor
3
Recorder
Removable Recording Media
5
6

FIGURE 2



GPS is GeoPositioning System
C-VIBE is the counter vibration unit
RPY is Roll-Pitch-Yaw detection
CAMID is Camera Identification
SeqNum is sequence number

(Parentheses refer to the Generic Signal Device Model)

FIGURE 2A

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 3 of 21

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/626,044	07/27/2000	Jonathan E. Jaffe	6468/78445	9426

7590 09/03/2003

Welsh & Katz
120 south Riverside Plaza
22nd Floor
Chicago, IL 60606

EXAMINER	
SONG, HOSUK	
ART UNIT	PAPER NUMBER
2131	3

DATE MAILED: 09/03/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

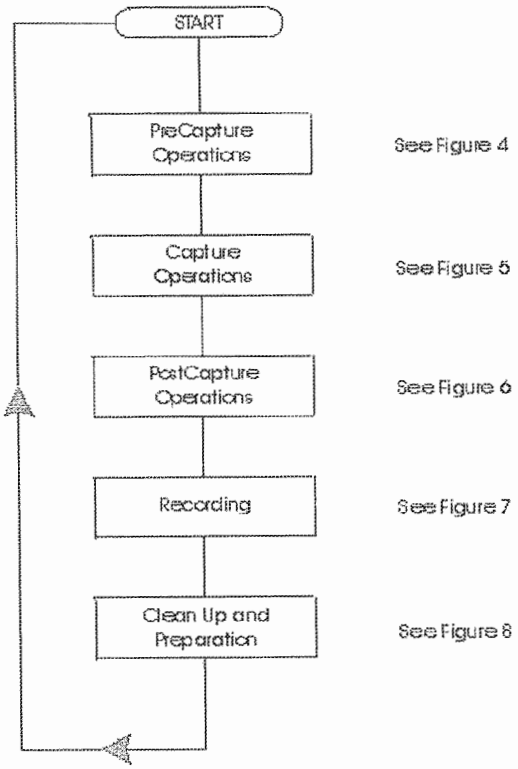

START
PreCapture Operations
See Figure 4
Capture Operations
See Figure 5
PostCapture Operations
See Figure 6
Recording
See Figure 7
Clean Up and Preparation
See Figure 8

FIGURE 3

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 4 of 21

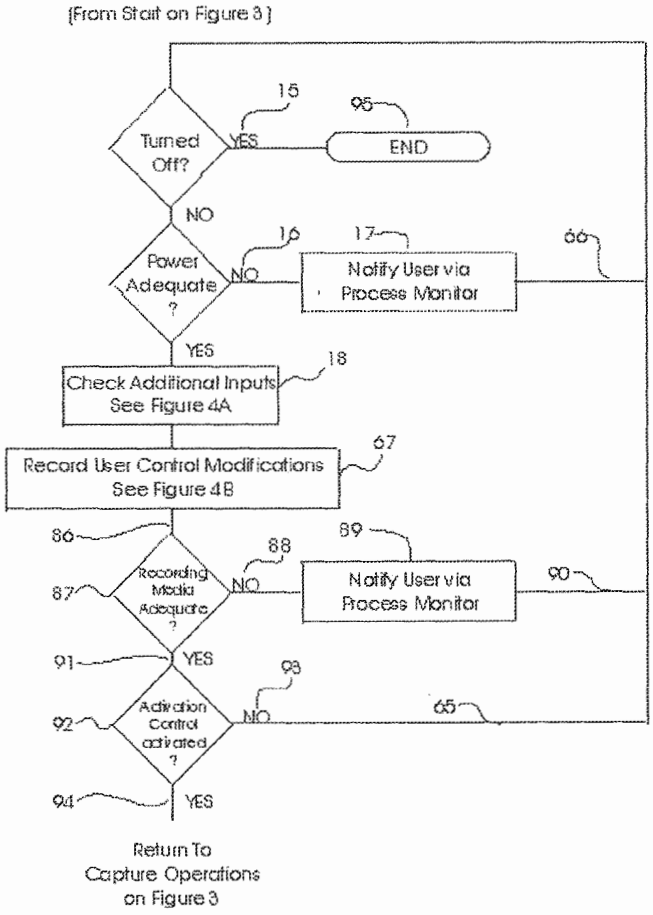
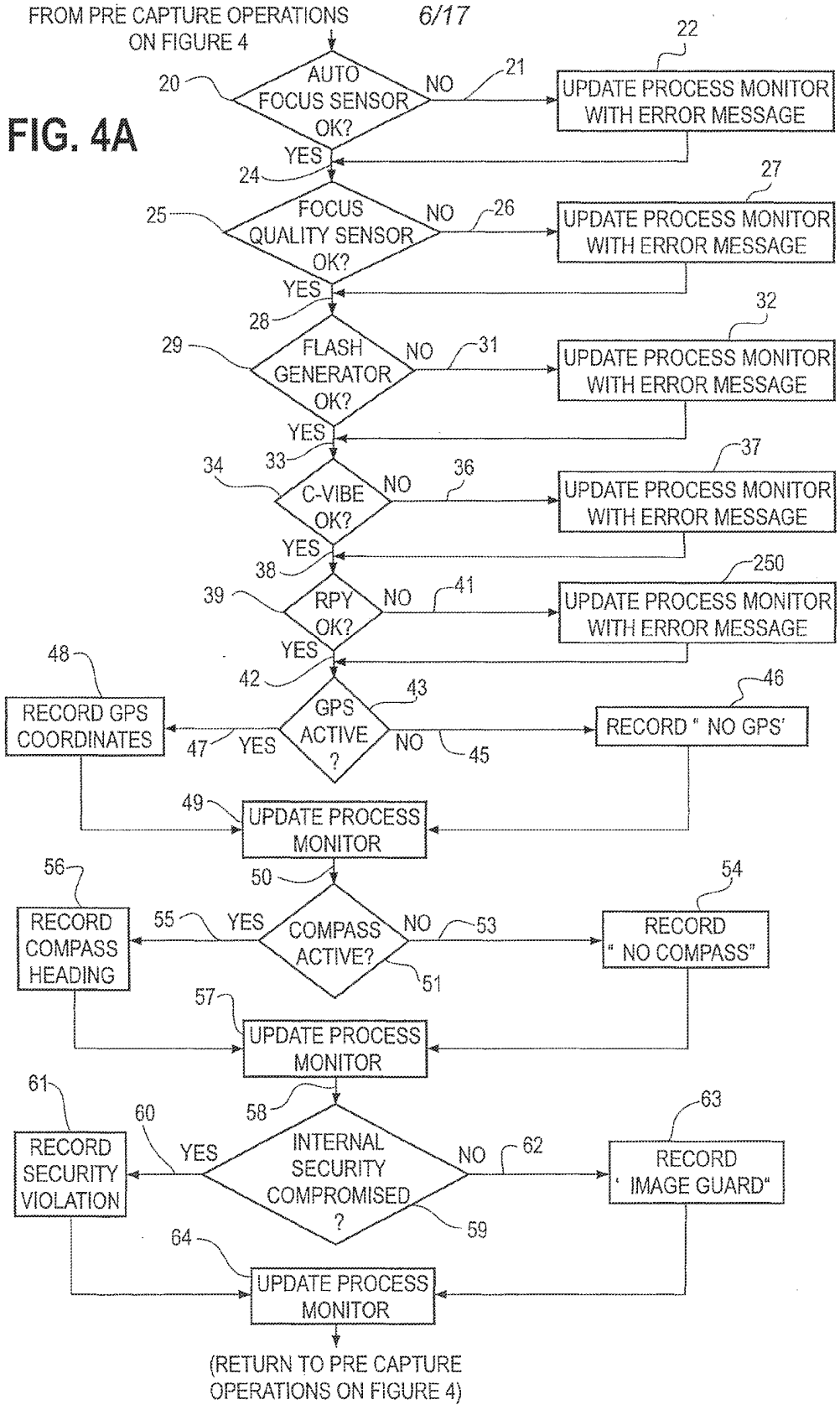

(From Start on Figure 3)
Turned Off?
15
YES
95
END
NO
Power Adequate ?
16
NO
17
Notify User via Process Monitor
66
YES
Check Additional Inputs See Figure 4A
18
Record User Control Modifications See Figure 4B
67
86
Recording Media Adequate ?
87
88
NO
89
Notify User via Process Monitor
90
91
YES
Activation Control activated ?
92
98
NO
65
94
YES
Return To Capture Operations on Figure 3

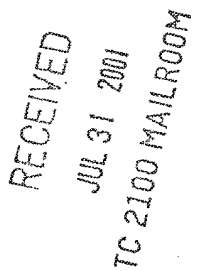
FIGURE 4

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 5 of 21

FIG. 4A

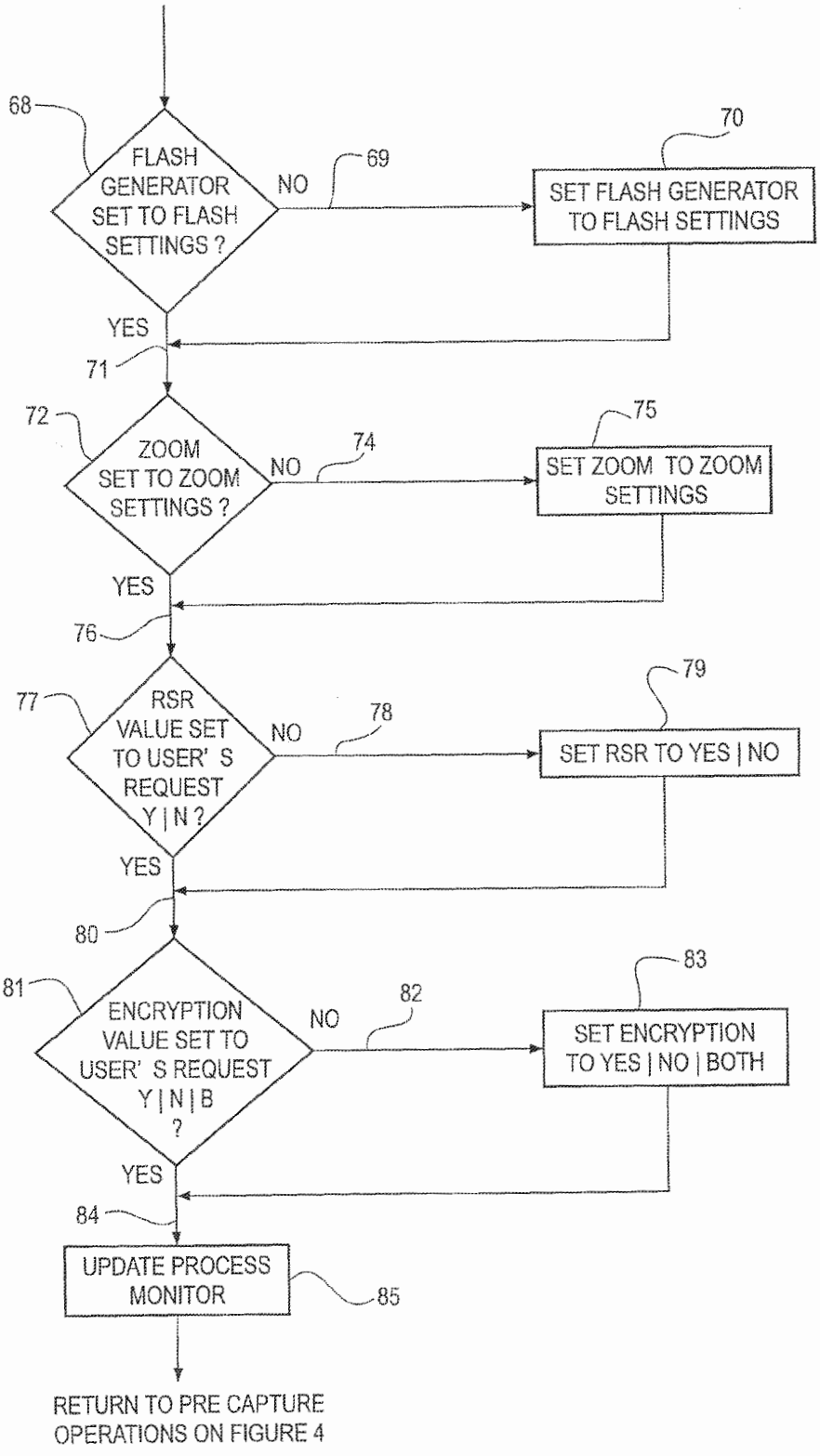

6/17
FROM PRE CAPTURE OPERATIONS ON FIGURE 4
AUTO FOCUS SENSOR OK?
NO
YES
UPDATE PROCESS MONITOR WITH ERROR MESSAGE
FOCUS QUALITY SENSOR OK?
FLASH GENERATOR OK?
C-VIBE OK?
RPY OK?
GPS ACTIVE ?
RECORD GPS COORDINATES
RECORD " NO GPS'
UPDATE PROCESS MONITOR
COMPASS ACTIVE?
RECORD COMPASS HEADING
RECORD " NO COMPASS"
INTERNAL SECURITY COMPROMISED ?
RECORD SECURITY VIOLATION
RECORD ' IMAGE GUARD"
(RETURN TO PRE CAPTURE OPERATIONS ON FIGURE 4)


OIPE
JC87
JUL 27 2001
PATENT & TRADEMARK OFFICE

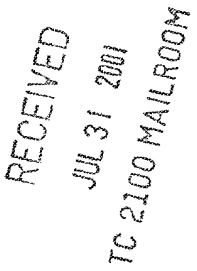

RECEIVED
JUL 31 2001
TC 2100 MAILROOM

7/17

FIG. 4B

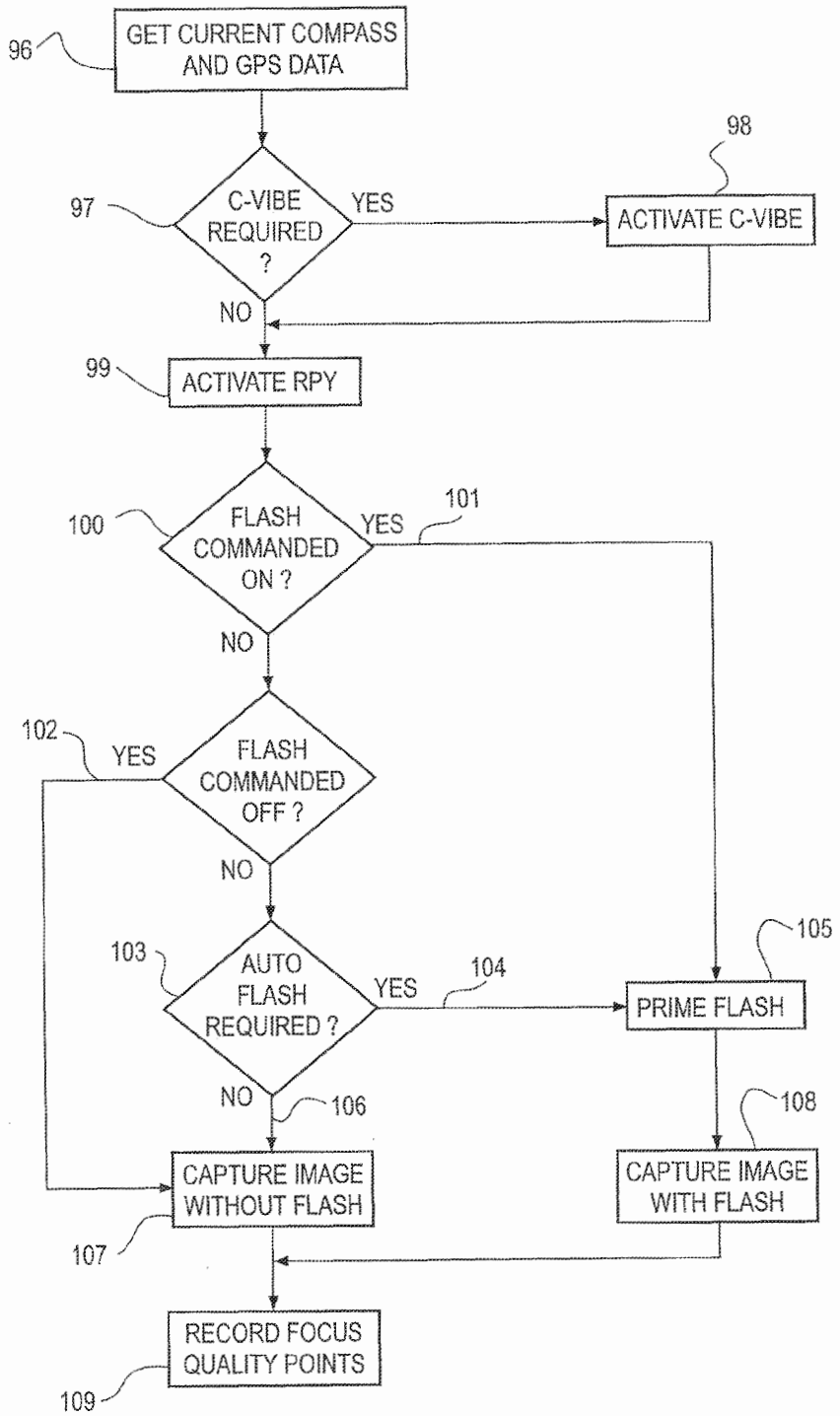

(FROM PRE CAPTURE OPERATIONS ON FIGURE 4)
68
FLASH GENERATOR SET TO FLASH SETTINGS ?
NO
69
70
SET FLASH GENERATOR TO FLASH SETTINGS
YES
71
72
ZOOM SET TO ZOOM SETTINGS ?
NO
74
75
SET ZOOM TO ZOOM SETTINGS
YES
76
77
RSR VALUE SET TO USER' S REQUEST Y | N ?
NO
78
79
SET RSR TO YES | NO
YES
80
81
ENCRYPTION VALUE SET TO USER' S REQUEST Y | N | B ?
NO
82
83
SET ENCRYPTION TO YES | NO | BOTH
YES
84
UPDATE PROCESS MONITOR
85
RETURN TO PRE CAPTURE OPERATIONS ON FIGURE 4


OIPE JC87
JUL 27 2001
PATENT & TRADEMARK OFFICE


RECEIVED
JUL 31 2001
TC 2100 MAILROOM

8/17

FIG. 5


96
GET CURRENT COMPASS AND GPS DATA
97
C-VIBE REQUIRED ?
YES
98
ACTIVATE C-VIBE
NO
99
ACTIVATE RPY
100
FLASH COMMANDED ON ?
YES
101
NO
102
YES
FLASH COMMANDED OFF ?
NO
103
AUTO FLASH REQUIRED ?
YES
104
105
PRIME FLASH
NO
106
108
CAPTURE IMAGE WITHOUT FLASH
CAPTURE IMAGE WITH FLASH
107
RECORD FOCUS QUALITY POINTS
109


OIPE
JC87
JUL 27 2001
PATENT & TRADEMARK OFFICE

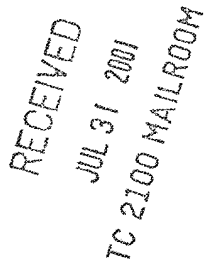
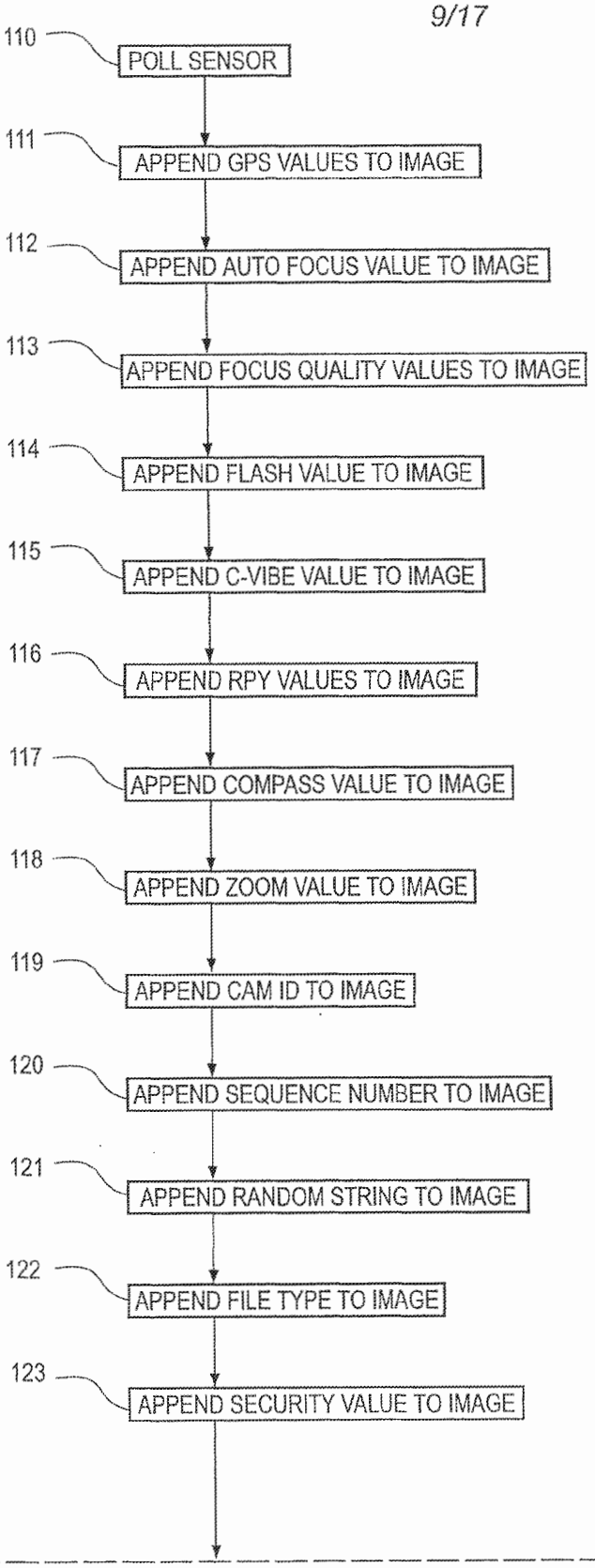
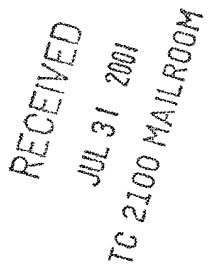

RECEIVED
JUL 31 2001
TC 2100 MAILROOM

FIG. 6A


110
POLL SENSOR
111
APPEND GPS VALUES TO IMAGE
112
APPEND AUTO FOCUS VALUE TO IMAGE
113
APPEND FOCUS QUALITY VALUES TO IMAGE
114
APPEND FLASH VALUE TO IMAGE
115
APPEND C-VIBE VALUE TO IMAGE
116
APPEND RPY VALUES TO IMAGE
117
APPEND COMPASS VALUE TO IMAGE
118
APPEND ZOOM VALUE TO IMAGE
119
APPEND CAM ID TO IMAGE
120
APPEND SEQUENCE NUMBER TO IMAGE
121
APPEND RANDOM STRING TO IMAGE
122
APPEND FILE TYPE TO IMAGE
123
APPEND SECURITY VALUE TO IMAGE


OIPE
JC67
JUL 27 2001
PATENT & TRADEMARK OFFICE


RECEIVED
JUL 31 2001
TC 2100 MAILROOM

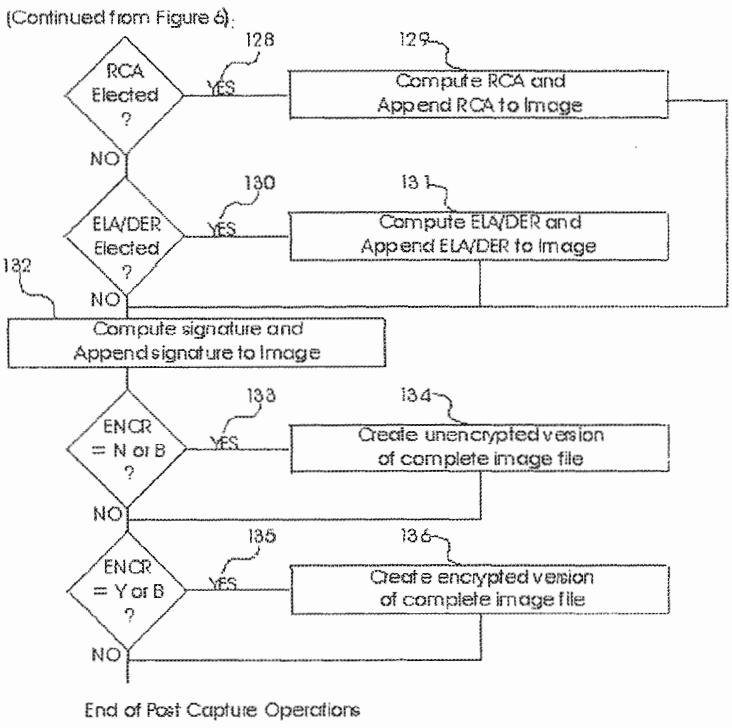

(Continued from Figure 6)
RCA Elected ?
128
YES
129
Compute RCA and Append RCA to Image
NO
ELA/DER Elected ?
130
YES
131
Compute ELA/DER and Append ELA/DER to Image
132
NO
Compute signature and Append signature to Image
ENCR = N or B ?
133
YES
134
Create unencrypted version of complete image file
NO
ENCR = Y or B ?
135
YES
136
Create encrypted version of complete image file
NO
End of Post Capture Operations

FIGURE 6

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 11 of 21

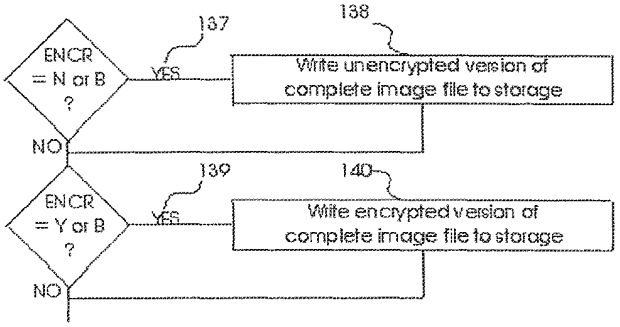

137
138
ENCR
= N or B
?
YES
Write unencrypted version of
complete image file to storage
NO
139
140
ENCR
= Y or B
?
YES
Write encrypted version of
complete image file to storage
NO
End of Recording Operations

FIGURE 7

5042.230 Issued

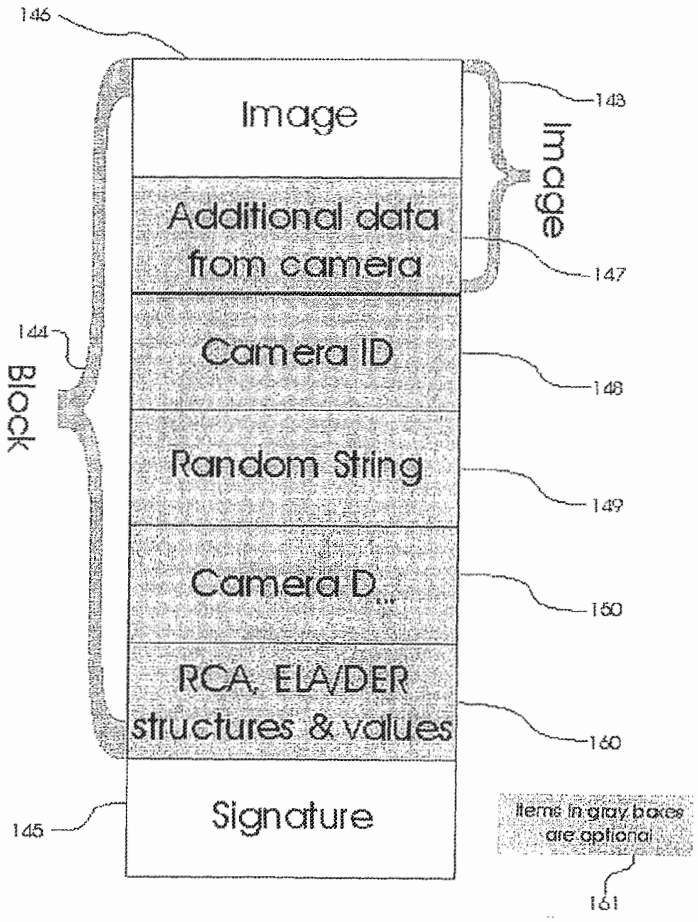


FIGURE 7A

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 13 of 21

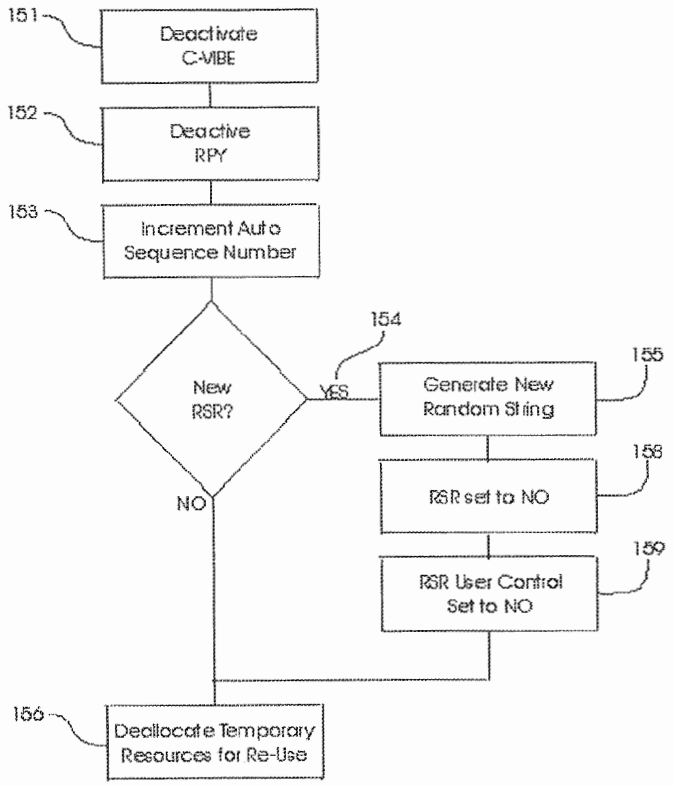

151
Deactivate C-VIBE
152
Deactive RPY
153
Increment Auto Sequence Number
154
New RSR?
YES
155
Generate New Random String
NO
158
RSR set to NO
159
RSR User Control Set to NO
156
Deallocate Temporary Resources for Re-Use

FIGURE 8

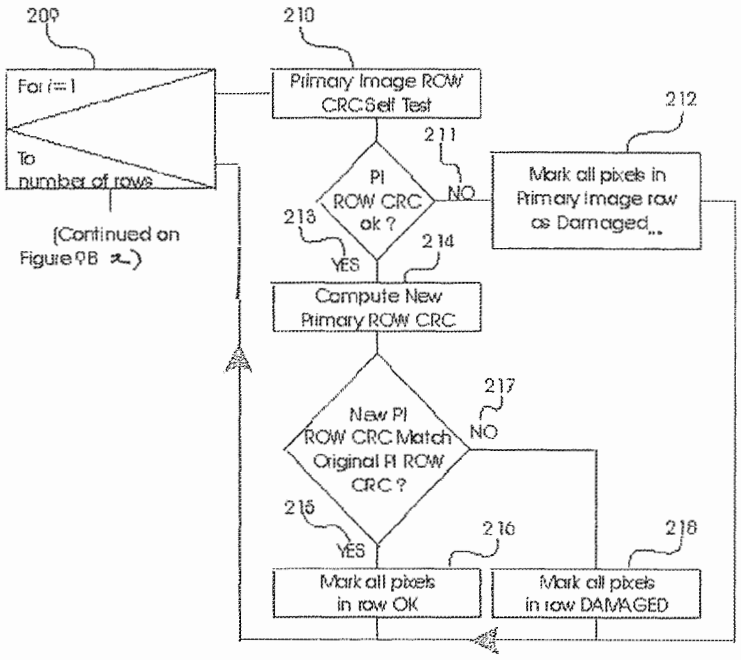

209
For i=1
To number of rows
(Continued on Figure 9B)
210
Primary Image ROW CRC Self Test
211
PI ROW CRC ok ?
NO
212
Mark all pixels in Primary Image row as Damaged
213
YES
214
Compute New Primary ROW CRC
217
New PI ROW CRC Match Original PI ROW CRC ?
NO
215
YES
216
Mark all pixels in row OK
218
Mark all pixels in row DAMAGED

FIGURE 9B

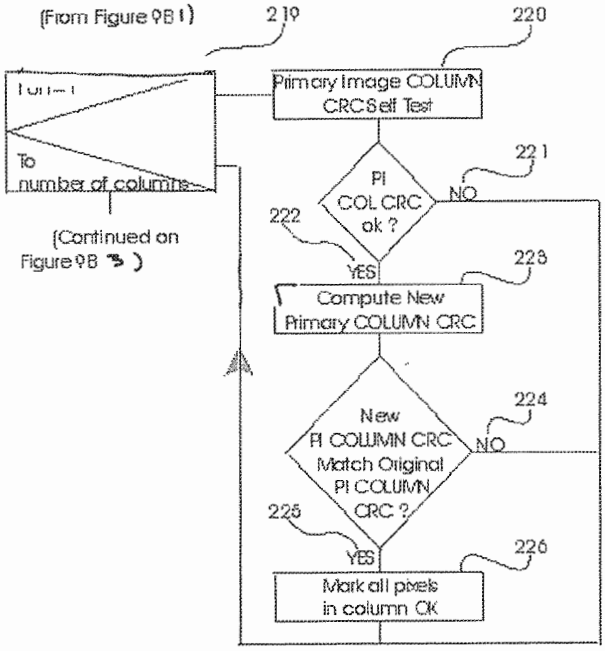

(From Figure 9B1)
219
220
Primary Image COLUMN CRC Self Test
To number of columns
(Continued on Figure 9B3)
PI COL CRC ok ?
221
NO
222
YES
223
Compute New Primary COLUMN CRC
New PI COLUMN CRC Match Original PI COLUMN CRC ?
224
NO
225
YES
226
Mark all pixels in column OK

FIGURE 9B2

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 19 of 21

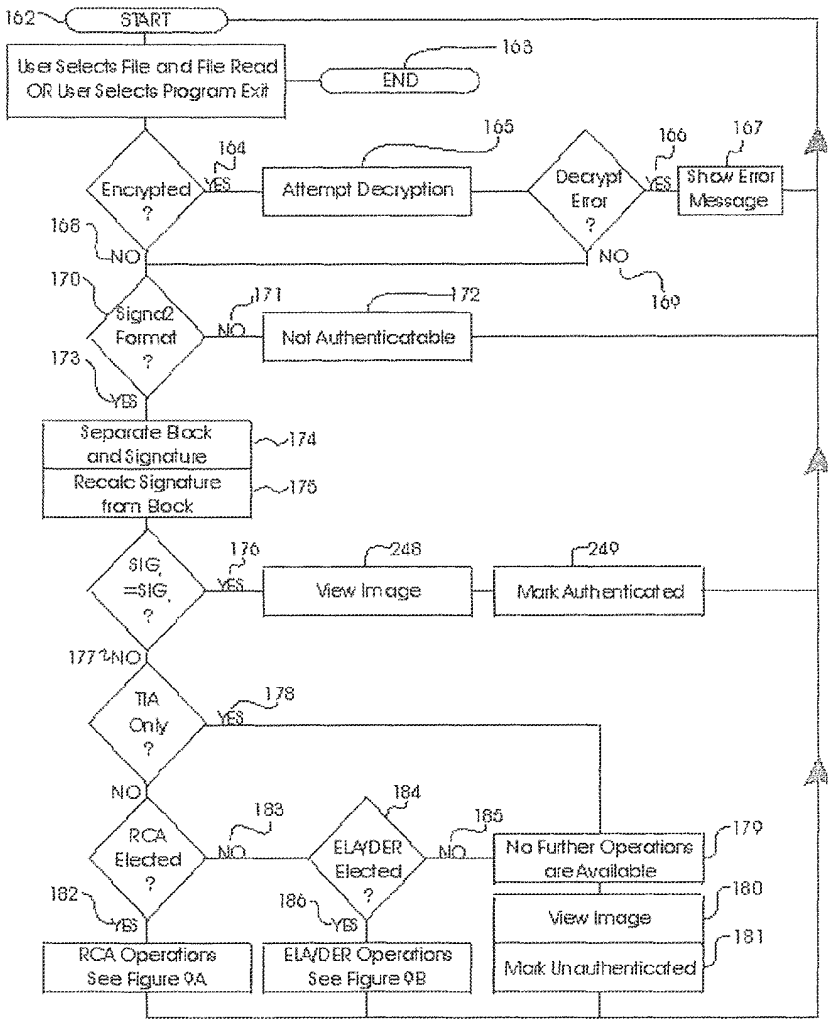
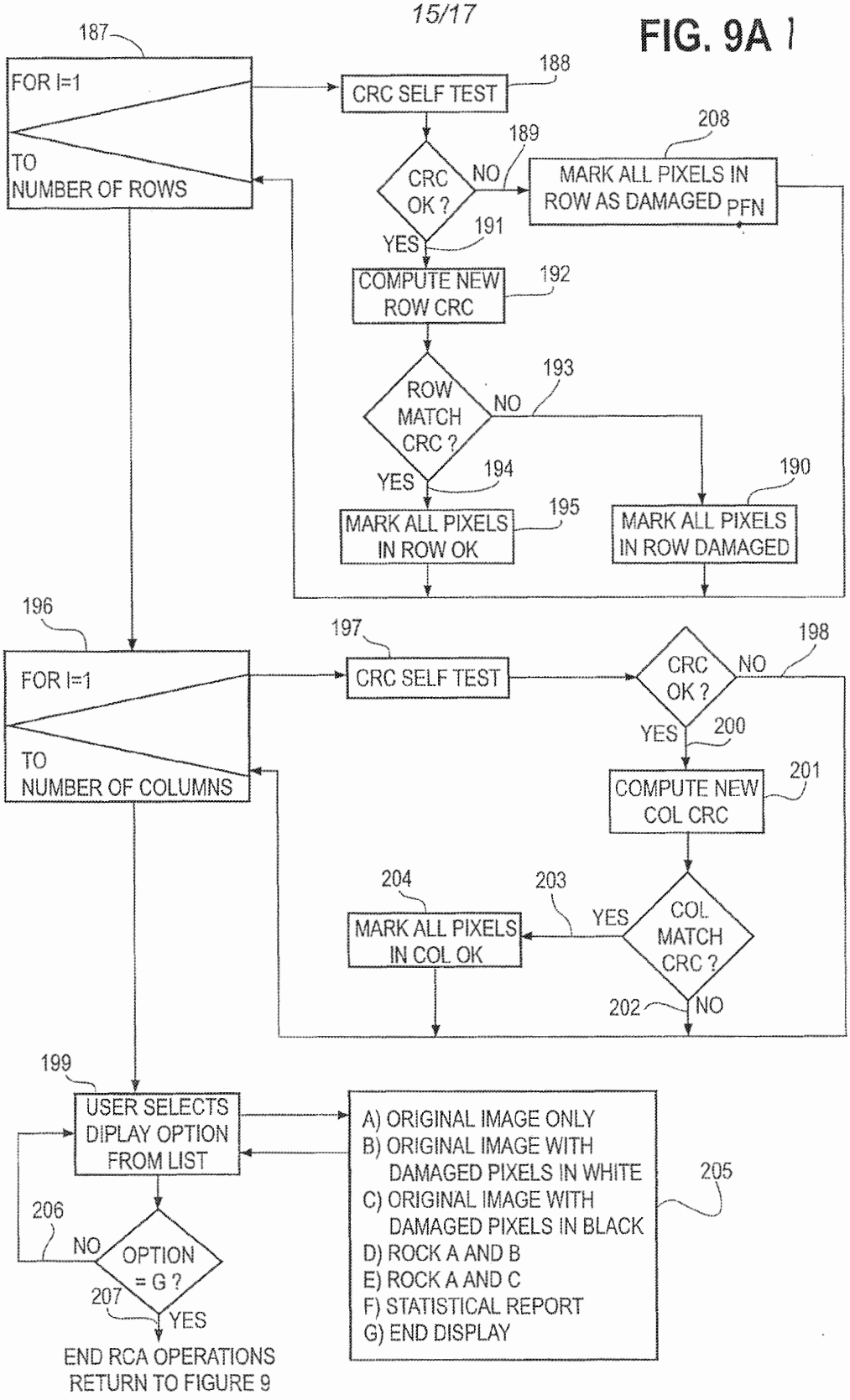

162
START
User Selects File and File Read
OR User Selects Program Exit
163
END
Encrypted ?
164
YES
165
Attempt Decryption
Decrypt Error ?
166
YES
167
Show Error Message
NO
168
NO
169
Signed Format ?
170
NO
171
172
Not Authenticatable
173
YES
Separate Block and Signature
174
Recalc Signature from Block
175
SIG1 =SIG2 ?
176
YES
248
View Image
249
Mark Authenticated
177
NO
TIA Only ?
178
YES
NO
RCA Elected ?
183
NO
184
ELA/DER Elected ?
185
NO
No Further Operations are Available
179
182
YES
186
YES
View Image
180
Mark Unauthenticated
181
RCA Operations See Figure 9A
ELA/DER Operations See Figure 9B

FIGURE 9

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 15 of 21

FIG. 9A 1


187
FOR I=1
TO
NUMBER OF ROWS
188
CRC SELF TEST
189
CRC OK ?
NO
208
MARK ALL PIXELS IN ROW AS DAMAGED PFN
YES
191
COMPUTE NEW ROW CRC
192
ROW MATCH CRC ?
193
NO
YES
194
MARK ALL PIXELS IN ROW OK
195
190
MARK ALL PIXELS IN ROW DAMAGED
196
FOR I=1
TO
NUMBER OF COLUMNS
197
CRC SELF TEST
CRC OK ?
198
NO
YES
200
COMPUTE NEW COL CRC
201
COL MATCH CRC ?
YES
203
204
MARK ALL PIXELS IN COL OK
202
NO
199
USER SELECTS DIPLAY OPTION FROM LIST
A) ORIGINAL IMAGE ONLY
B) ORIGINAL IMAGE WITH DAMAGED PIXELS IN WHITE
C) ORIGINAL IMAGE WITH DAMAGED PIXELS IN BLACK
D) ROCK A AND B
E) ROCK A AND C
F) STATISTICAL REPORT
G) END DISPLAY
205
206
NO
OPTION = G ?
207
YES
END RCA OPERATIONS
RETURN TO FIGURE 9



RECEIVED
JUL 31 2001
TC 2100 MAILROOM

PRINT OF DRAWINGS
AS ORIGINALLY FILED

300/200

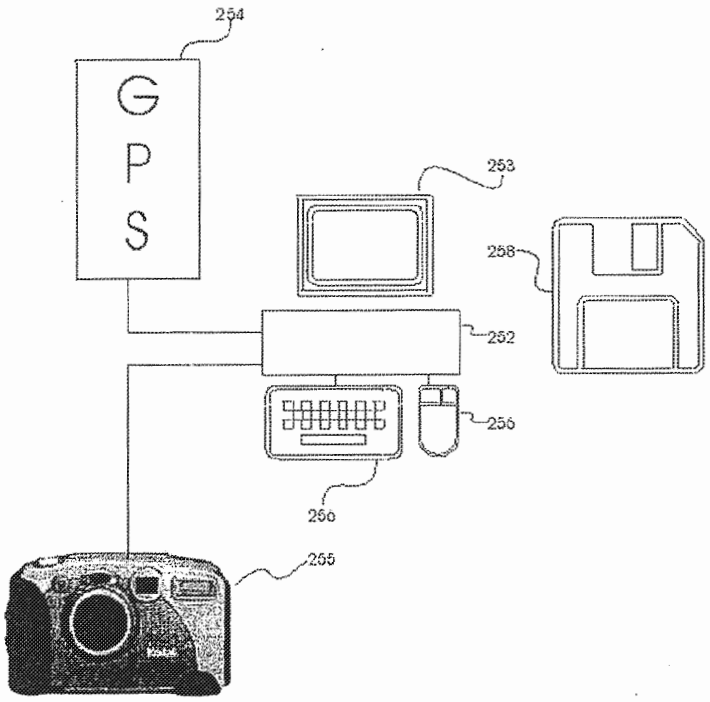


FIGURE 1

PRINT OF DRAWINGS
AS ORIGINALLY FILED

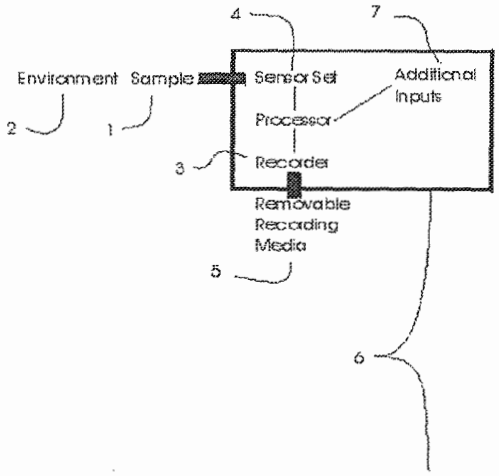
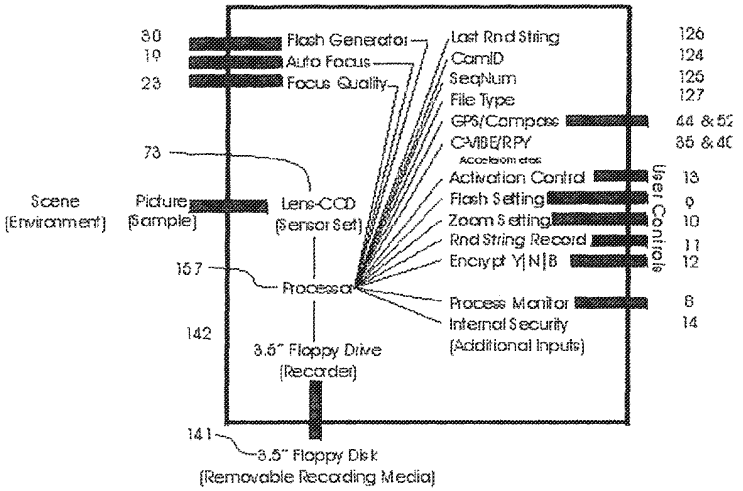


FIGURE 2

PRINT OF DRAWINGS
AS ORIGINALLY FILED



GPS is GeoPositioning System
CMBE is the counter vibration unit
RPY is Roll-Pitch-Yaw detection
CAMID is Camera Identification
SeqNum is sequence number

(Parentheses refer to the Generic Signal Device Model)

FIGURE 2A

PRINT OF DRAWINGS
AS ORIGINALLY FILED

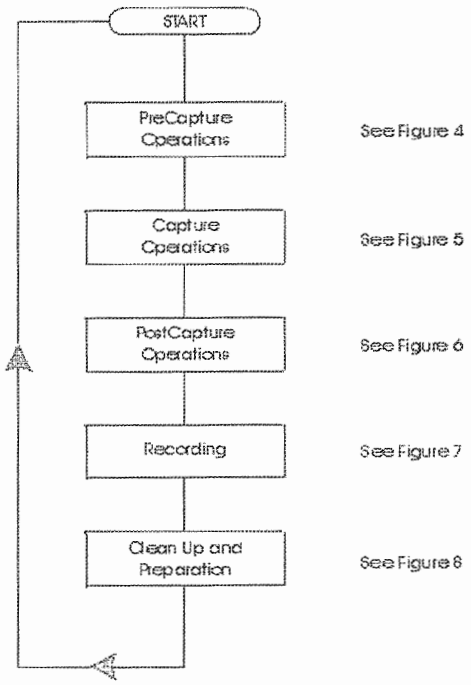


FIGURE 3

PRINT OF DRAWINGS
AS ORIGINALLY FILED

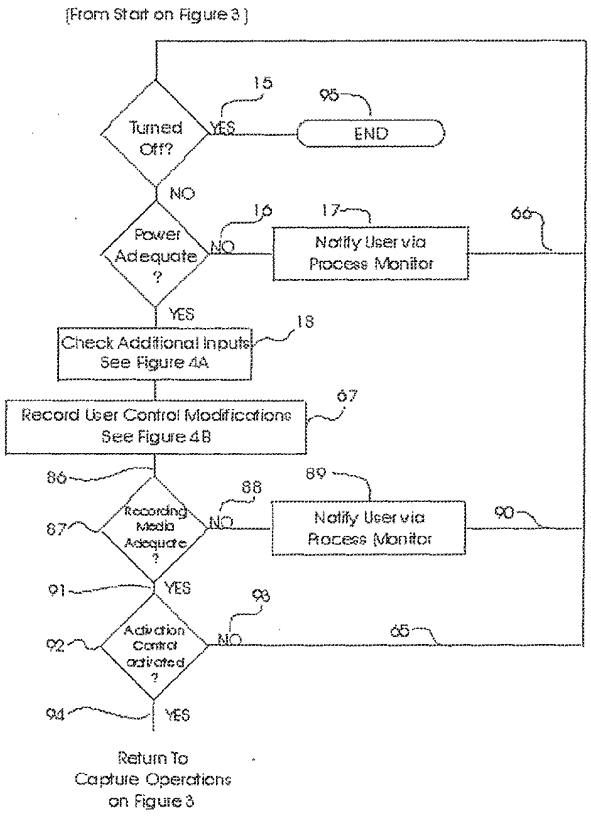


FIGURE 4

PRINT OF DRAWINGS
AS ORIGINALLY FILED

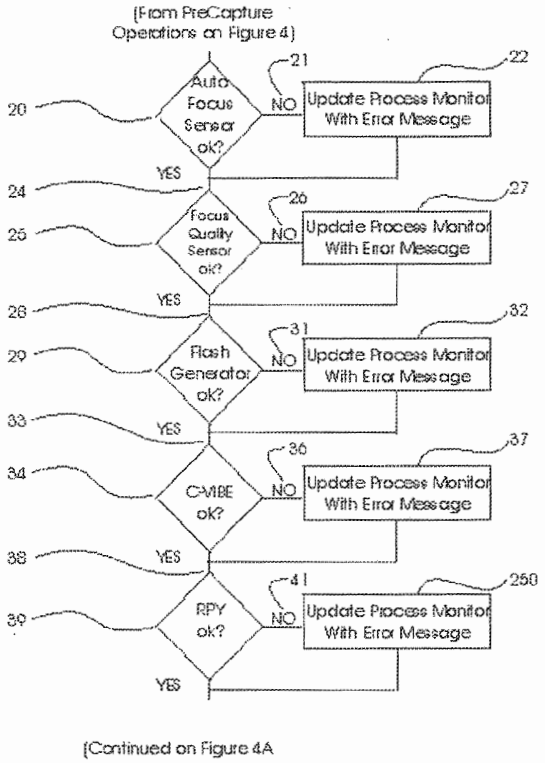


FIGURE 4A

PRINT OF DRAWINGS
AS ORIGINALLY FILED

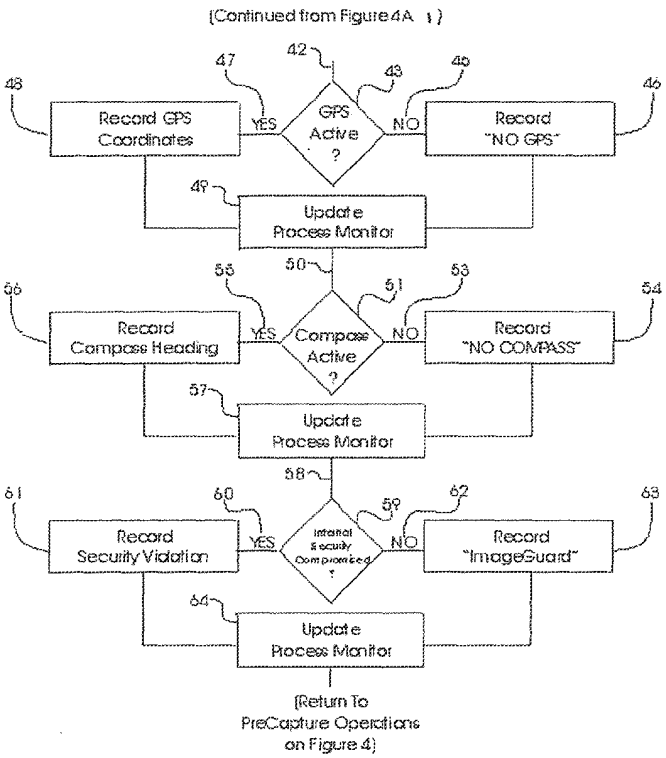


FIGURE 4A2

PRINT OF DRAWINGS
AS ORIGINALLY FILED

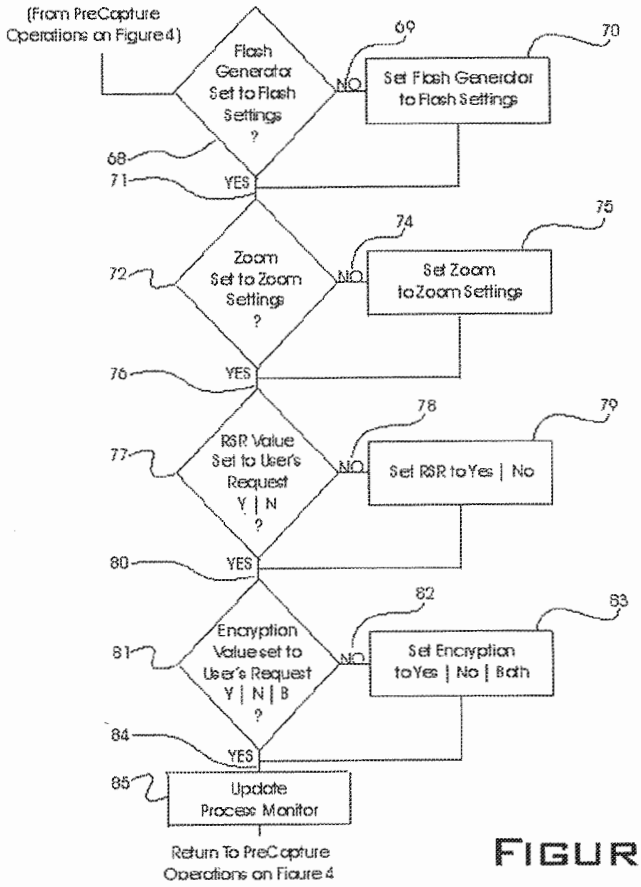


FIGURE 4B

PRINT OF DRAWINGS
AS ORIGINALLY FILED

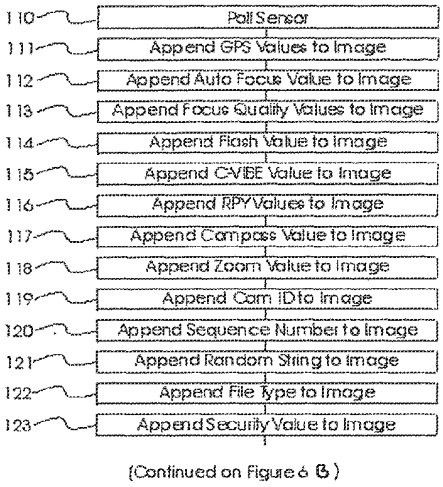


FIGURE 6

PRINT OF DRAWINGS
AS ORIGINALLY FILED

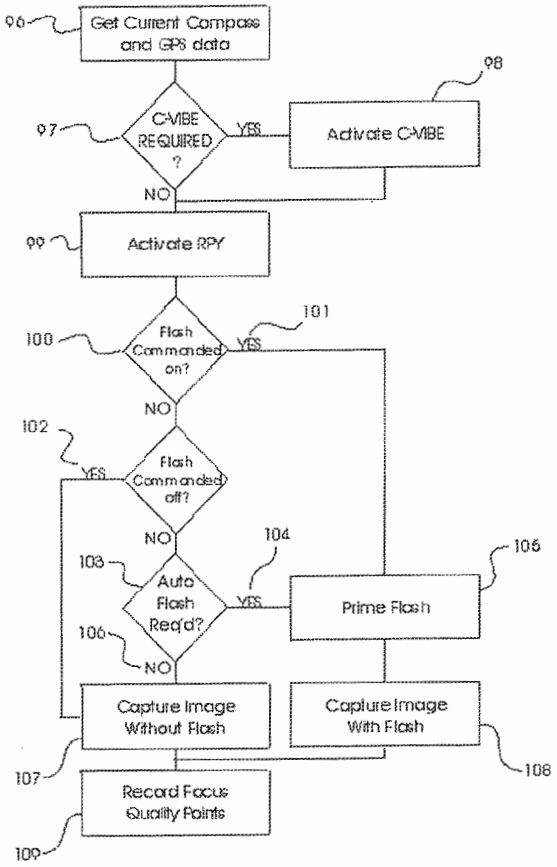


FIGURE 5

PRINT OF DRAWINGS
AS ORIGINALLY FILED

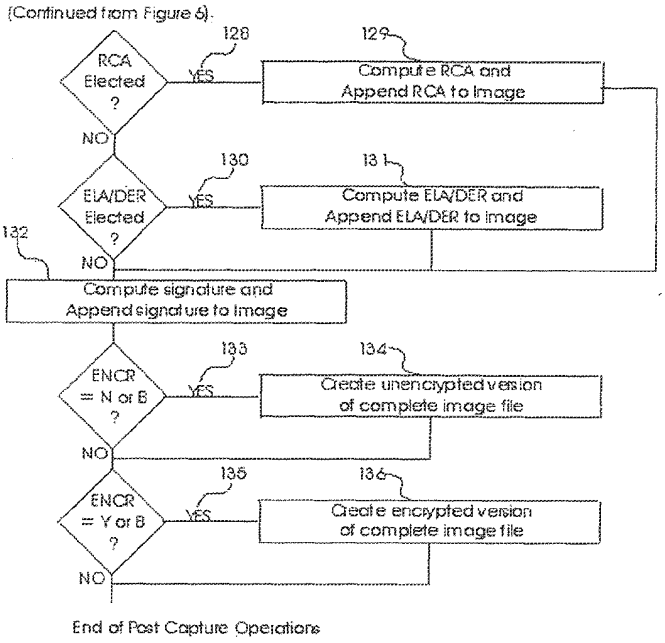


FIGURE 6

PRINT OF DRAWINGS
AS ORIGINALLY FILED

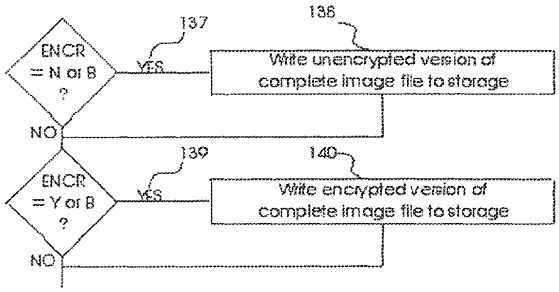


FIGURE 7

PRINT OF DRAWINGS
AS ORIGINALLY FILED

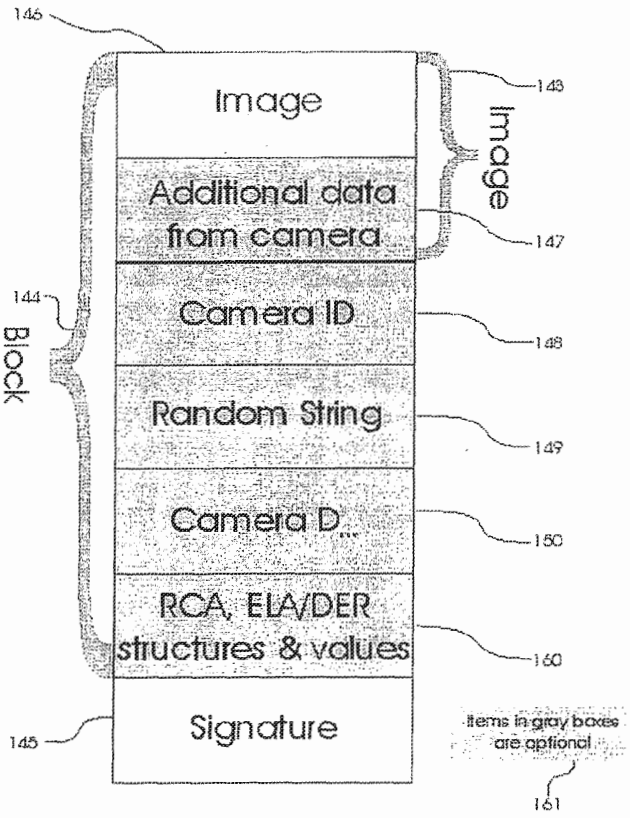


FIGURE 7A

PRINT OF DRAWINGS
AS ORIGINALLY FILED

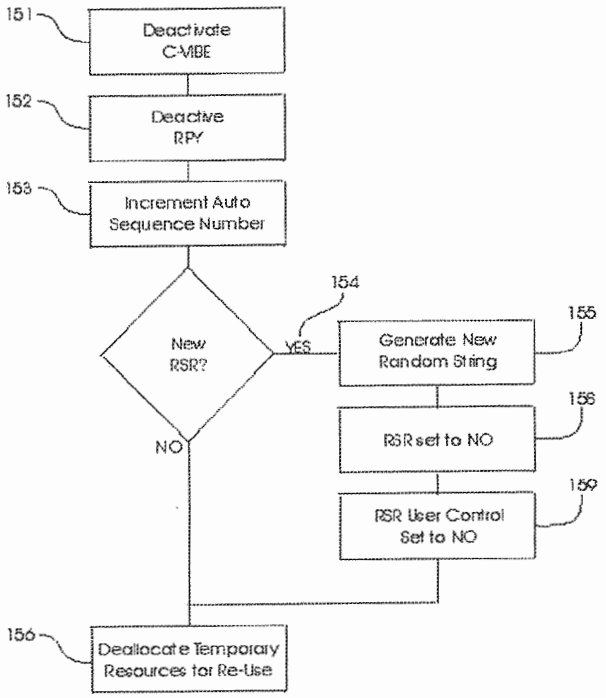


FIGURE 8

PRINT OF DRAWINGS
AS ORIGINALLY FILED

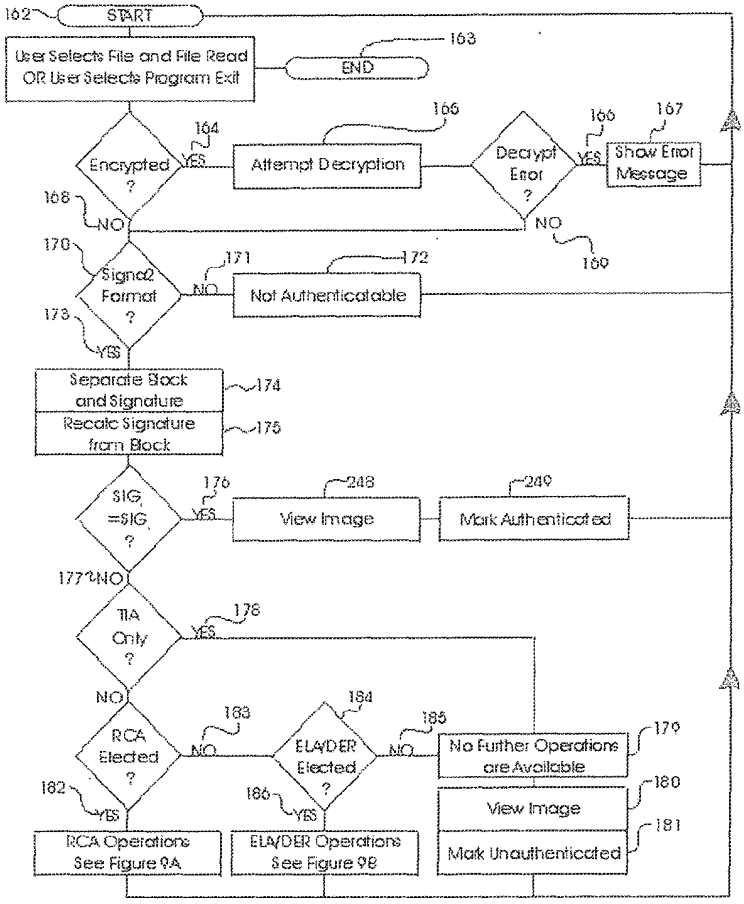


FIGURE 9

PRINT OF DRAWINGS
AS ORIGINALLY FILED

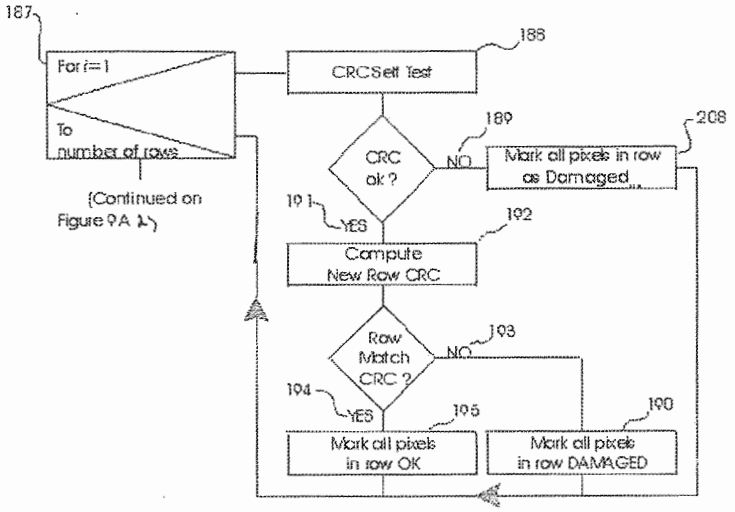


FIGURE 9A1

PRINT OF DRAWINGS
AS ORIGINALLY FILED

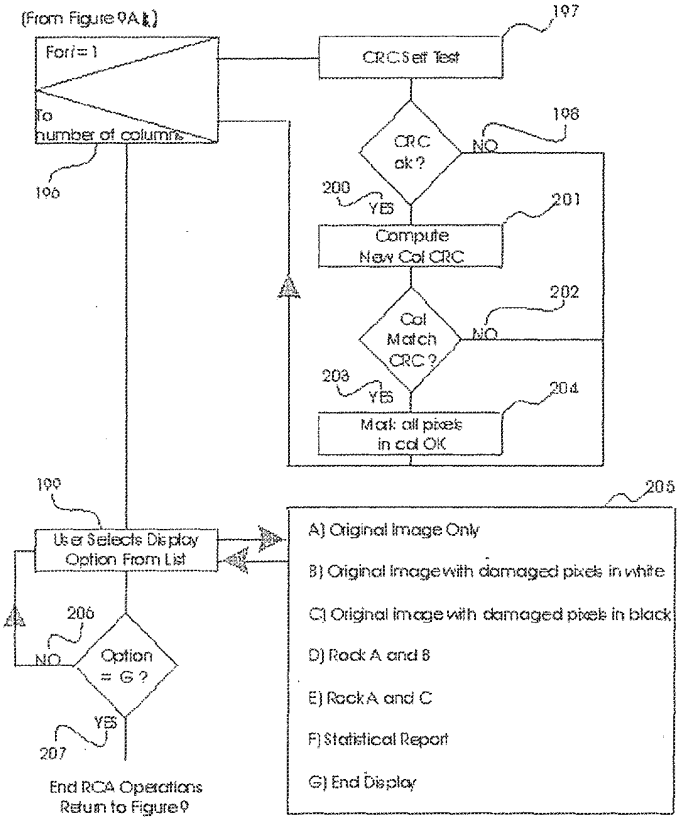


FIGURE 9A2

PRINT OF DRAWINGS
AS ORIGINALLY FILED

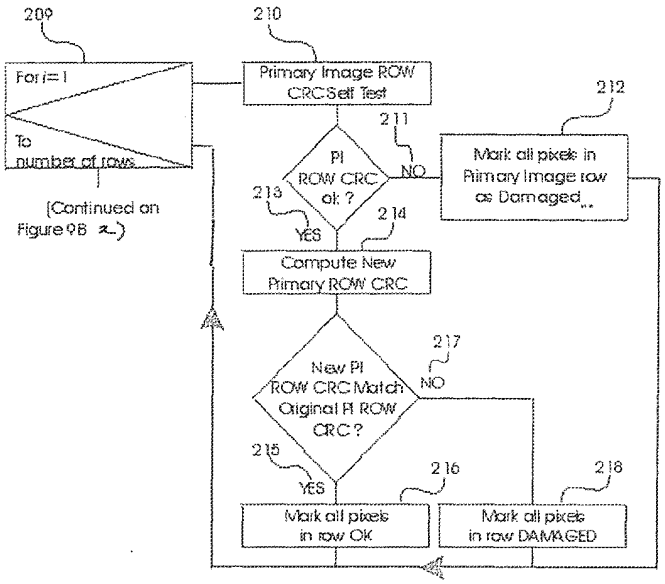


FIGURE 9B

PRINT OF DRAWINGS
AS ORIGINALLY FILED

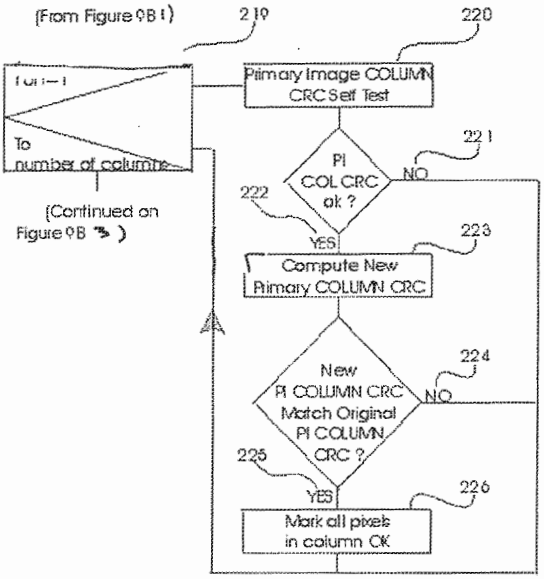


FIGURE 9B2

PRINT OF DRAWINGS
AS ORIGINALLY FILED

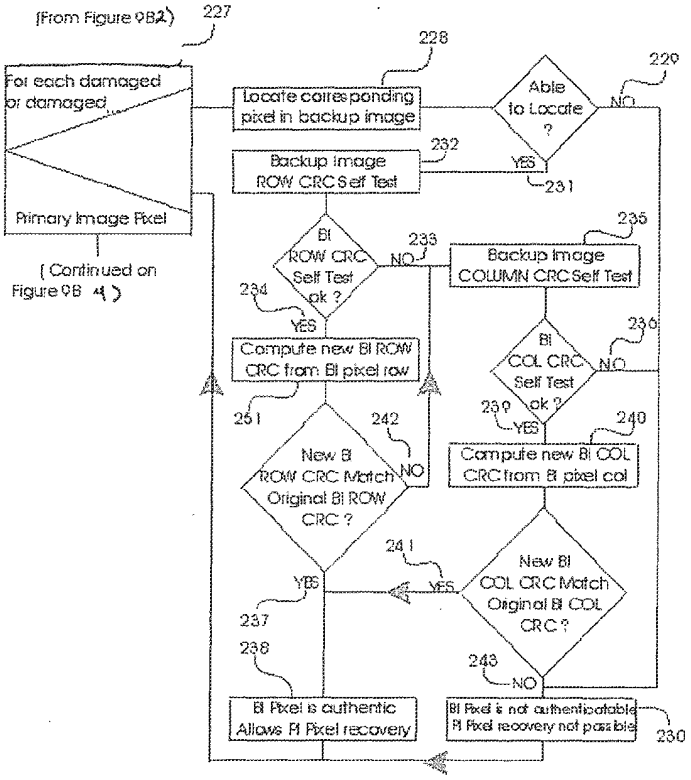


FIGURE 9B3

PRINT OF DRAWINGS
AS ORIGINALLY FILED

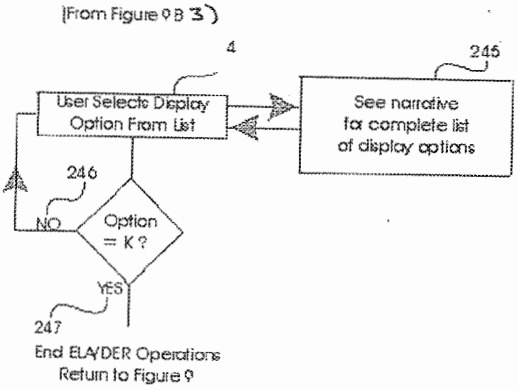


FIGURE 9B4

GAU 2766

2131

JUL 27 2001

Please type a plus sign (+) inside this box ☐ +

PTO/SB/21 (6-98)
Approved for use through 09/30/2000. OMB 0651-0031
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 FORM

(to be used for all correspondence after initial filing)

Application Number	09626,044
Filing Date	July 27, 2000
First Named Inventor	*Jonathan E. Jaffe et al.*
Group Art Unit	2766
Examiner Name	Not yet assigned
Total Number of Pages in This Submission	
Attorney Docket Number	6468/78445

RECEIVED
JUL 31 2001
TC 2100 MAILROOM

ENCLOSURES *(check all that apply)*

- ☐ Fee Transmittal Form
- ☐ Fee Attached
- ☐ Amendment/Response
- ☐ After Final
- ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/Incomplete Application
- ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Assignment Papers (for an Application)
- ☒ Drawing(s) (17 sheets)
- ☐ Licensing-related Papers
- ☐ Petition Routing Slip (PTO/SB/69) and Accompanying Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Small Entity Statement
- ☐ Request for Refund
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group *(Appeal Notices, Brief, Reply Brief)*
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Additional Enclosure(s) *(please identify below):*
  - ☒ **Submission of Formal Drawings**
  - ☒ Return Postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual Name	Jeffrey W. Salmon, Esq. (Reg. No. 37,435)
Signature	Jeffrey W. Salmon
Date	July 26, 2001

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope Addressed to: Box Official Draftsman; Commissioner for Patents, Washington, DC 20231 on this date: 07/25/01

Typed or Printed Name	Jeffrey W. Salmon, Esq. (Reg. No. 37,435)		
Signature	Jeffrey W. Salmon	Date 7/25/01	July 25, 2001

+ Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Office, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

OIPE JC87
JUL 27 2001
PATENT & TRADEMARK OFFICE

#12
8-2-01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	*Jonathan E. Jaffe et al.*	Group No.:	2766
Serial No.:	09/626,044	Examiner:	Not yet assigned
Filed:	July 27, 2000		
For:	INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES		
Attorney Docket No.:	6468/78445		

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Box Official Draftsman; Commissioner for Patents; Washington, D.C. 20231 on this date:

07/25/2001 Date — Signature

Drawings approved 8/9/01

RECEIVED
JUL 31 2001
TC 2100 MAILROOM

SUBMISSION OF FORMAL DRAWINGS

Box OFFICIAL DRAFTSMAN
Commissioner for Patents
Washington, DC 20231
Attn: Official Draftsperson

Sir:

Submitted herewith are seventeen (17) sheets of formal drawings to be filed in the above-identified patent application. No new matter is added by the enclosed formal drawings.

Respectfully submitted,

WELSH & KATZ, LTD.

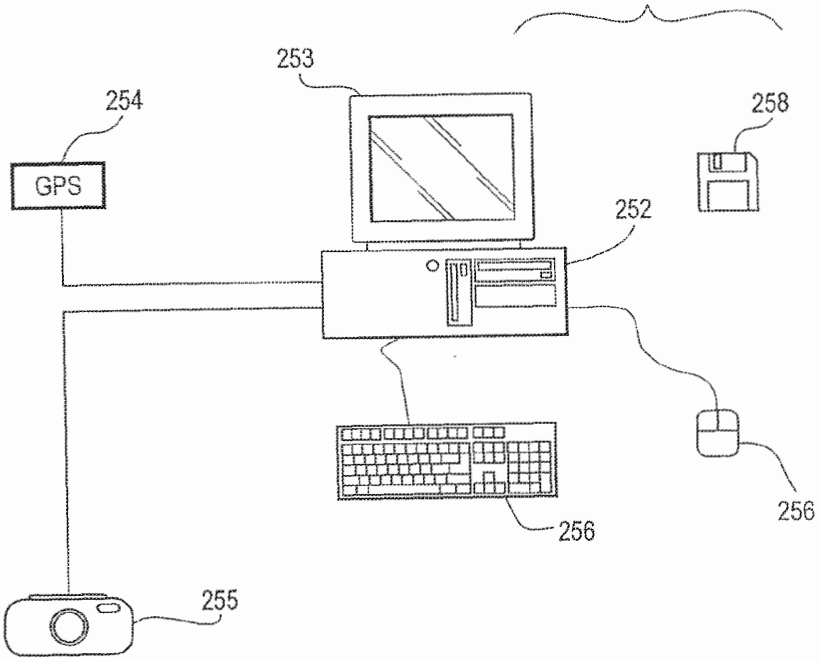
By: _____
Jeffrey W. Salmon
Registration No. 37,435

Dated: July 25, 2001
WELSH & KATZ, LTD.
120 South Riverside Plaza
22nd Floor
Chicago, IL 60606
(312) 655-1500

1/17

6757828

FIG. 1

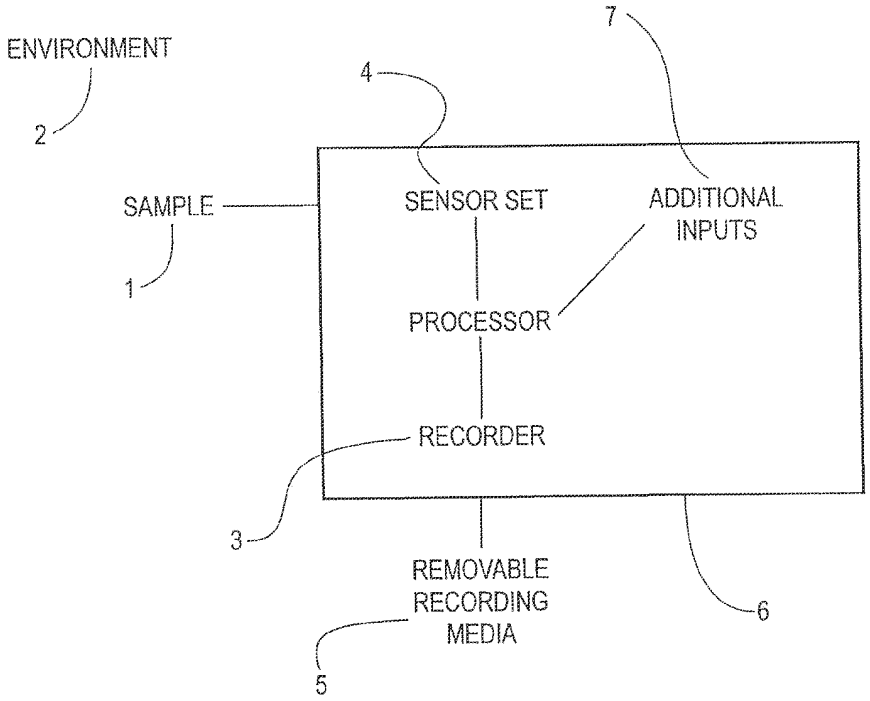




RECEIVED
JUL 31 2001
TC 2100 MAILROOM

2/17

FIG. 2

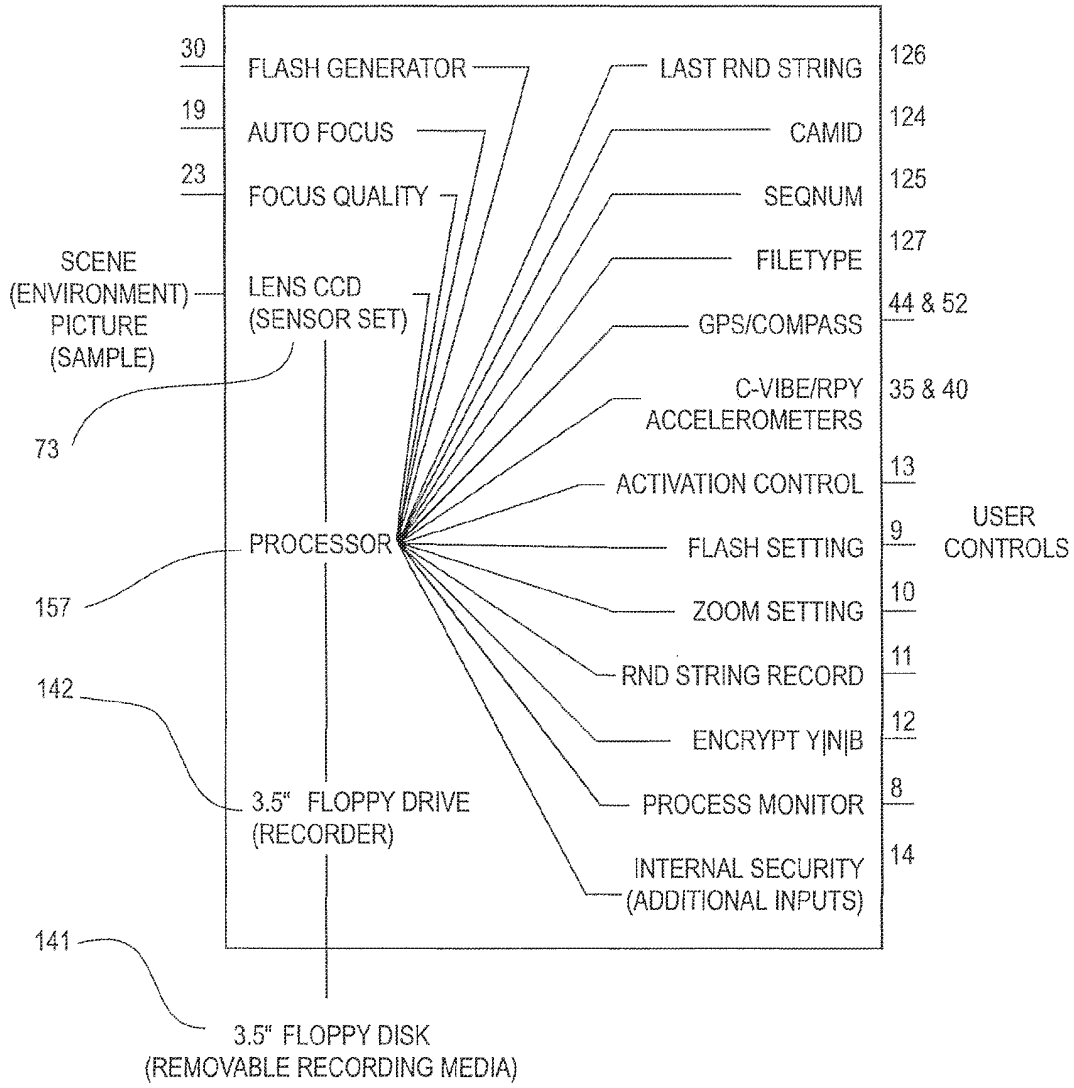

ENVIRONMENT
2
4
7
SAMPLE
1
SENSOR SET
ADDITIONAL INPUTS
PROCESSOR
RECORDER
3
REMOVABLE RECORDING MEDIA
5
6



RECEIVED
JUL 31 2001
TC 2100 MAILROOM

3/17

FIG. 2A



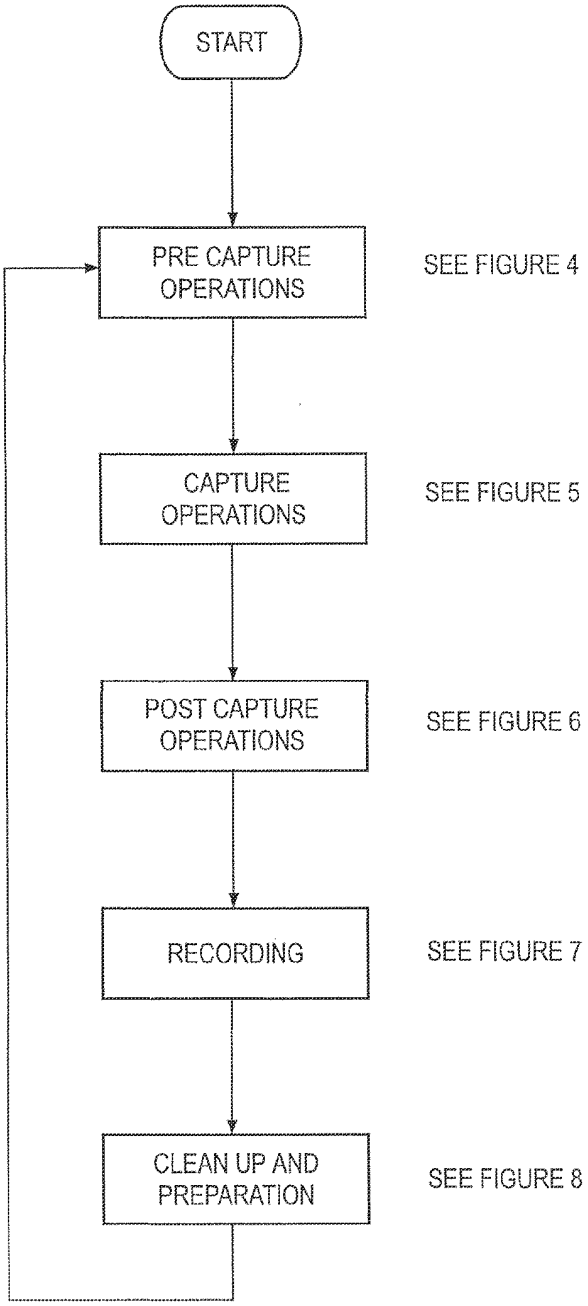
GPS IS GEOPOSITIONING SYSTEM
C-VIBE IS THE COUNTER VIBRATION UNIT
RPY IS ROLL-PITCH YAW DETECTION
CAMID IS CAMERA IDENTIFICATION
SEQNUM IS SEQUENCE NUMBER

OIPE JC8
JUL 27 2001
PATENT & TRADEMARK OFFICE

RECEIVED
JUL 31 2001
TC 2100 MAILROOM

4/17

FIG. 3

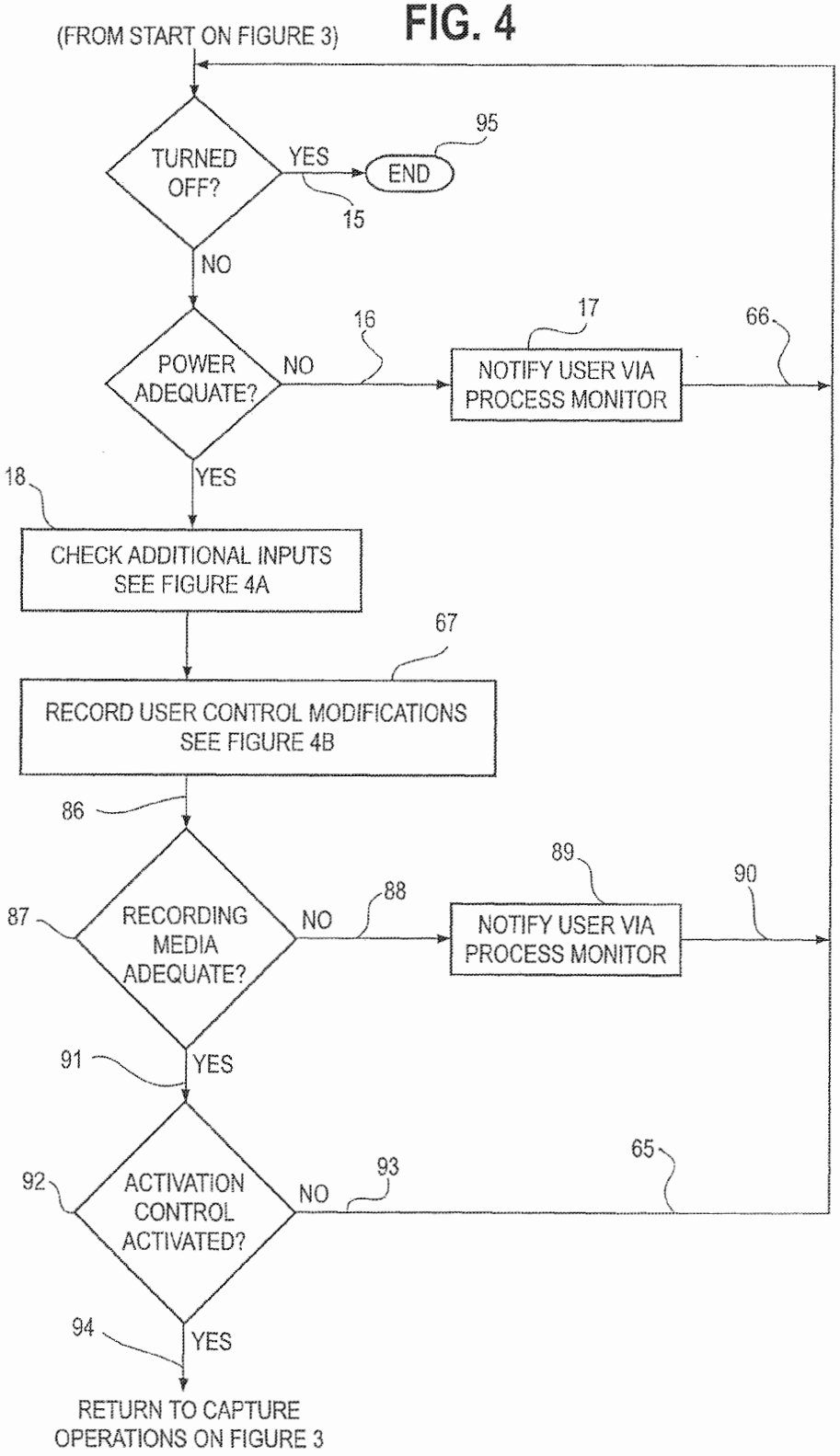

START
PRE CAPTURE OPERATIONS
SEE FIGURE 4
CAPTURE OPERATIONS
SEE FIGURE 5
POST CAPTURE OPERATIONS
SEE FIGURE 6
RECORDING
SEE FIGURE 7
CLEAN UP AND PREPARATION
SEE FIGURE 8

RECEIVED
JUL 31 2001
TC 2100 MAILROOM

OIPE JC87
PATENT & TRADEMARK OFFICE
JUL 27 2001

5/17

FIG. 4


(FROM START ON FIGURE 3)
TURNED OFF?
YES
95
END
15
NO
POWER ADEQUATE?
NO
16
17
NOTIFY USER VIA PROCESS MONITOR
66
YES
18
CHECK ADDITIONAL INPUTS SEE FIGURE 4A
67
RECORD USER CONTROL MODIFICATIONS SEE FIGURE 4B
86
RECORDING MEDIA ADEQUATE?
87
NO
88
89
NOTIFY USER VIA PROCESS MONITOR
90
91
YES
ACTIVATION CONTROL ACTIVATED?
92
NO
93
65
94
YES
RETURN TO CAPTURE OPERATIONS ON FIGURE 3


OIPE
JC87
JUL 27 2001
PATENT & TRADEMARK OFFICE


RECEIVED
JUL 31 2001
TC 2100 MAILROOM

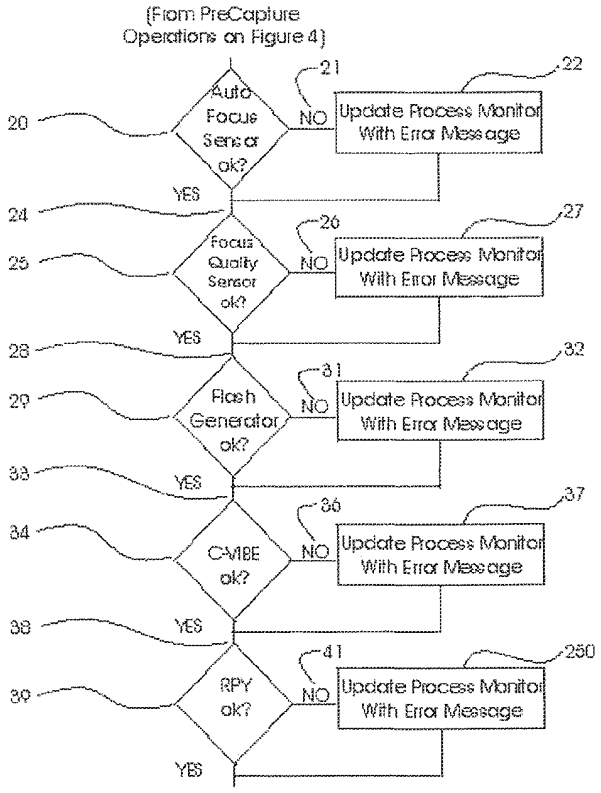

(From PreCapture Operations on Figure 4)
Auto Focus Sensor ok?
NO
Update Process Monitor With Error Message
YES
Focus Quality Sensor ok?
NO
Update Process Monitor With Error Message
YES
Flash Generator ok?
NO
Update Process Monitor With Error Message
YES
C-VIBE ok?
NO
Update Process Monitor With Error Message
YES
RPY ok?
NO
Update Process Monitor With Error Message
YES
20
21
22
24
25
26
27
28
29
31
32
33
34
36
37
38
39
41
250
(Continued on Figure 4A

FIGURE 4A

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 6 of 21

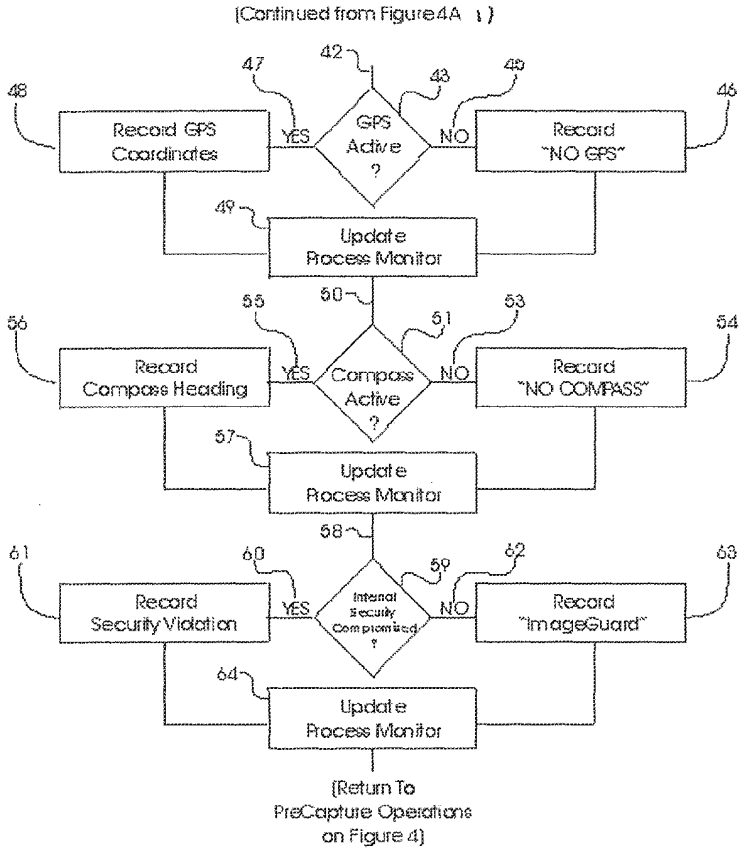

(Continued from Figure 4A 1)
42
47
43
48
Record GPS Coordinates
YES
GPS Active ?
NO
Record "NO GPS"
46
49
Update Process Monitor
50
55
51
53
56
Record Compass Heading
YES
Compass Active ?
NO
Record "NO COMPASS"
54
57
Update Process Monitor
58
61
60
59
62
63
Record Security Violation
YES
Internal Security Compromised ?
NO
Record "ImageGuard"
64
Update Process Monitor
(Return To PreCapture Operations on Figure 4)

FIGURE 4A2

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 7 of 21

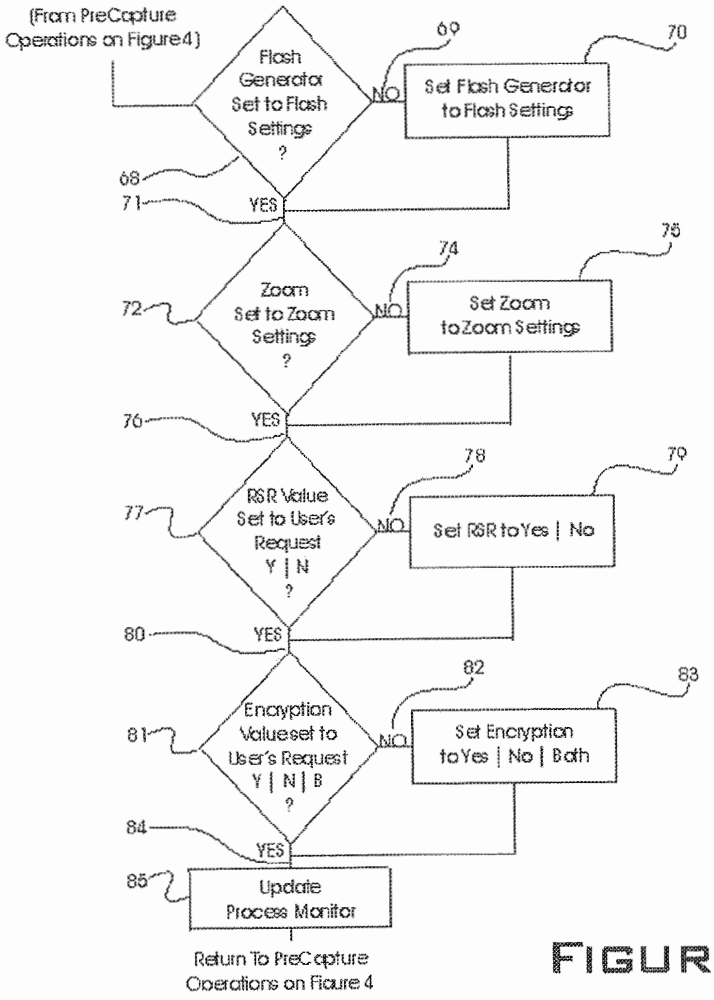

(From PreCapture Operations on Figure 4)
Flash Generator Set to Flash Settings ?
NO
69
70
Set Flash Generator to Flash Settings
68
71
YES
Zoom Set to Zoom Settings ?
NO
74
75
Set Zoom to Zoom Settings
72
76
YES
RSR Value Set to User's Request Y | N ?
NO
78
79
Set RSR to Yes | No
77
80
YES
Encryption Value set to User's Request Y | N | B ?
NO
82
83
Set Encryption to Yes | No | Both
81
84
YES
Update Process Monitor
85
Return To PreCapture Operations on Figure 4

FIGURE 4B

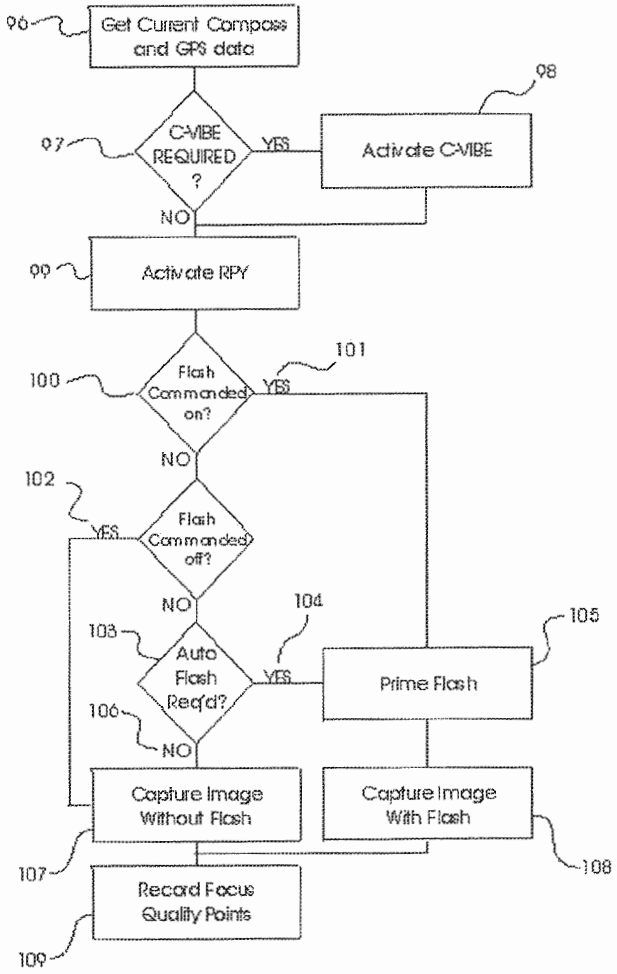

96
Get Current Compass and GPS data
98
97
C-VIBE REQUIRED ?
YES
Activate C-VIBE
NO
99
Activate RPY
101
100
Flash Commanded on?
YES
NO
102
YES
Flash Commanded off?
NO
104
105
103
Auto Flash Req'd?
YES
Prime Flash
106
NO
Capture Image Without Flash
Capture Image With Flash
108
107
Record Focus Quality Points
109

FIGURE 5

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 9 of 21

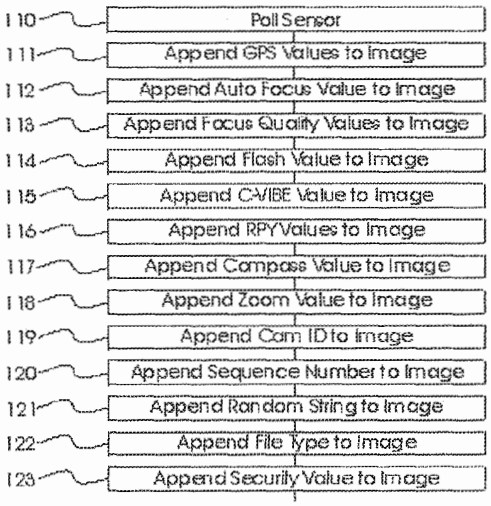
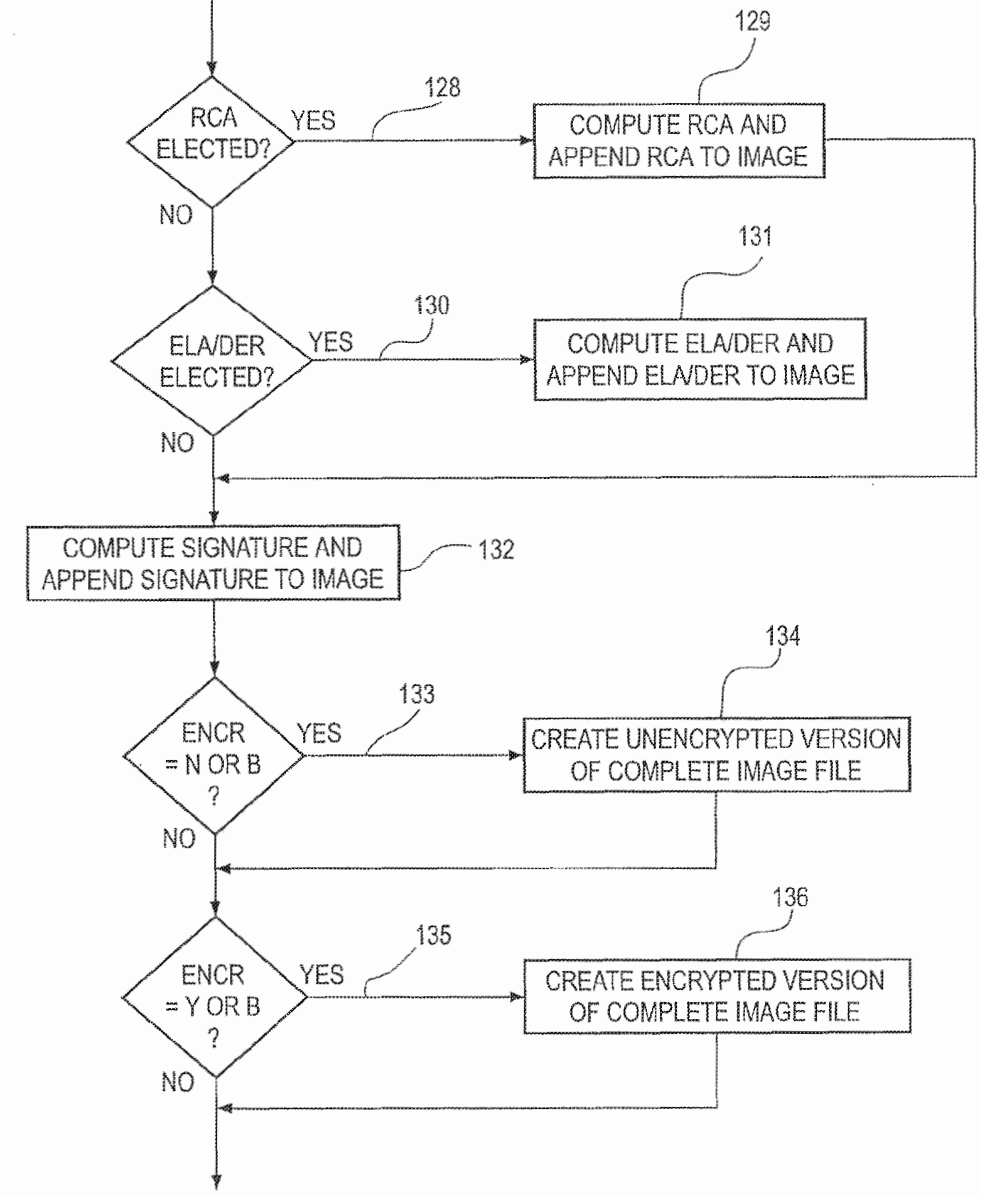

110
Poll Sensor
111
Append GPS Values to Image
112
Append Auto Focus Value to Image
113
Append Focus Quality Values to Image
114
Append Flash Value to Image
115
Append C-VIBE Value to Image
116
Append RPY Values to Image
117
Append Compass Value to Image
118
Append Zoom Value to Image
119
Append Cam ID to Image
120
Append Sequence Number to Image
121
Append Random String to Image
122
Append File Type to Image
123
Append Security Value to Image
(Continued on Figure 6 B)

FIGURE 6

FIG. 6B


RCA ELECTED?
YES
128
129
COMPUTE RCA AND APPEND RCA TO IMAGE
NO
ELA/DER ELECTED?
YES
130
131
COMPUTE ELA/DER AND APPEND ELA/DER TO IMAGE
NO
COMPUTE SIGNATURE AND APPEND SIGNATURE TO IMAGE
132
ENCR = N OR B ?
YES
133
134
CREATE UNENCRYPTED VERSION OF COMPLETE IMAGE FILE
NO
ENCR = Y OR B ?
YES
135
136
CREATE ENCRYPTED VERSION OF COMPLETE IMAGE FILE
NO
END OF POST CAPTURE OPERATIONS

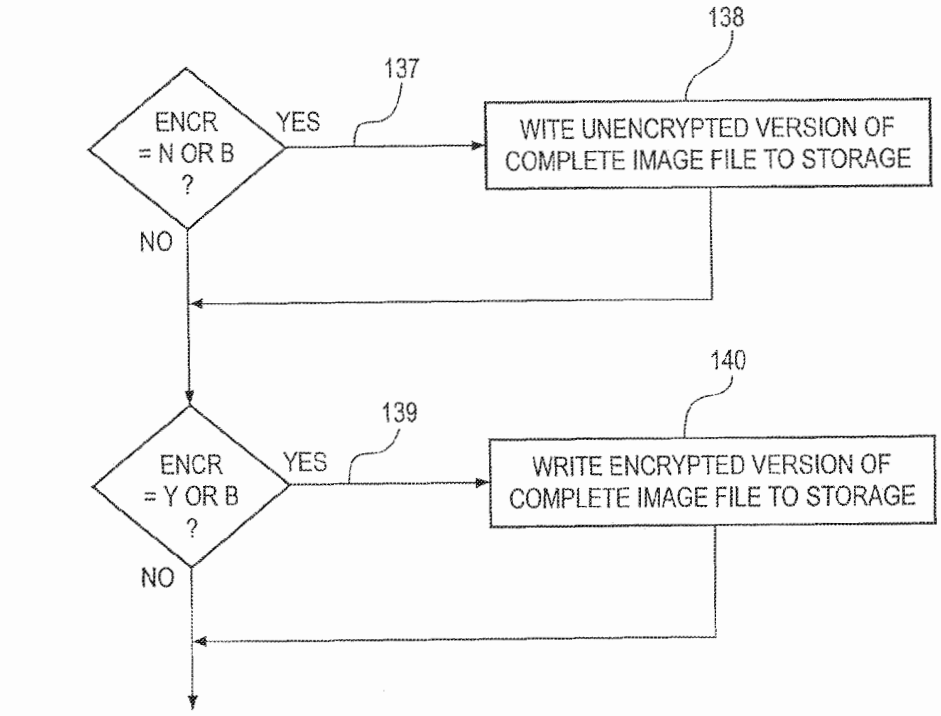
RECEIVED
JUL 31 2001
TC 2100 MAILROOM



JAFFE-ADOBE00164

11/11

FIG. 7


138
137
ENCR = N OR B ?
YES
WITE UNENCRYPTED VERSION OF COMPLETE IMAGE FILE TO STORAGE
NO
140
139
ENCR = Y OR B ?
YES
WRITE ENCRYPTED VERSION OF COMPLETE IMAGE FILE TO STORAGE
NO
END OF RECORDING OPERATIONS

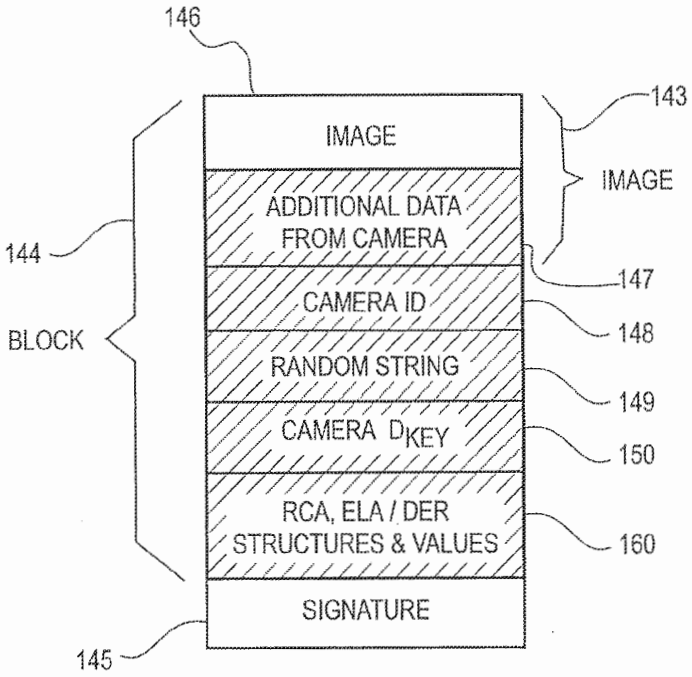
RECEIVED
JUL 31 2001
TC 2100 MAILROOM

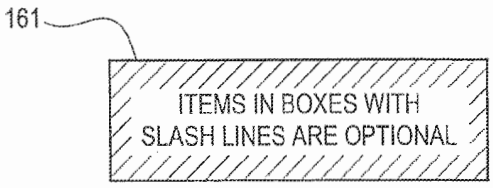


JAFFE-AD

12/17

FIG. 7A

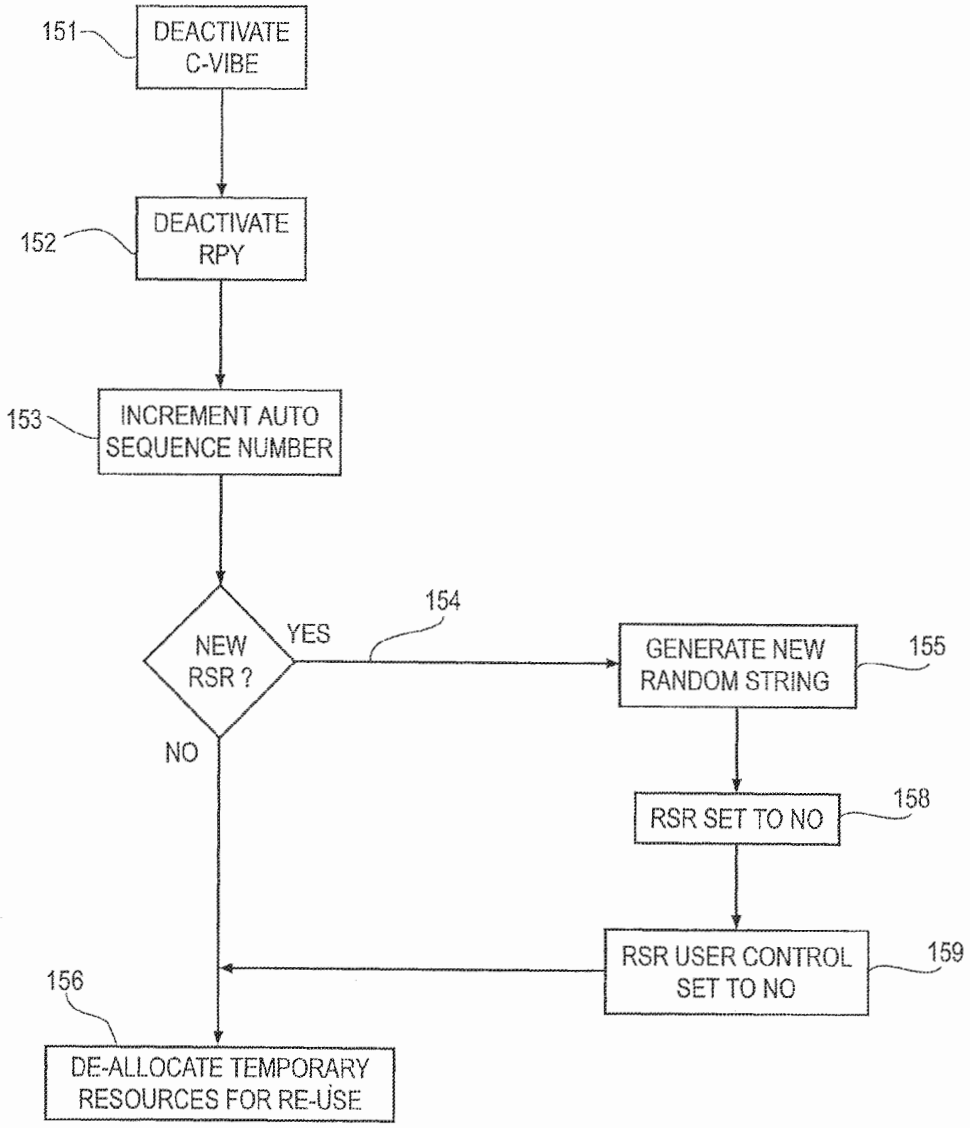

146
143
IMAGE
IMAGE
ADDITIONAL DATA FROM CAMERA
144
147
CAMERA ID
148
BLOCK
RANDOM STRING
149
CAMERA D_{KEY}
150
RCA, ELA / DER STRUCTURES & VALUES
160
SIGNATURE
145


161
ITEMS IN BOXES WITH SLASH LINES ARE OPTIONAL

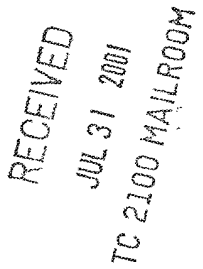


RECEIVED
JUL 31 2001
TC 2100 MAILROOM

FIG. 8

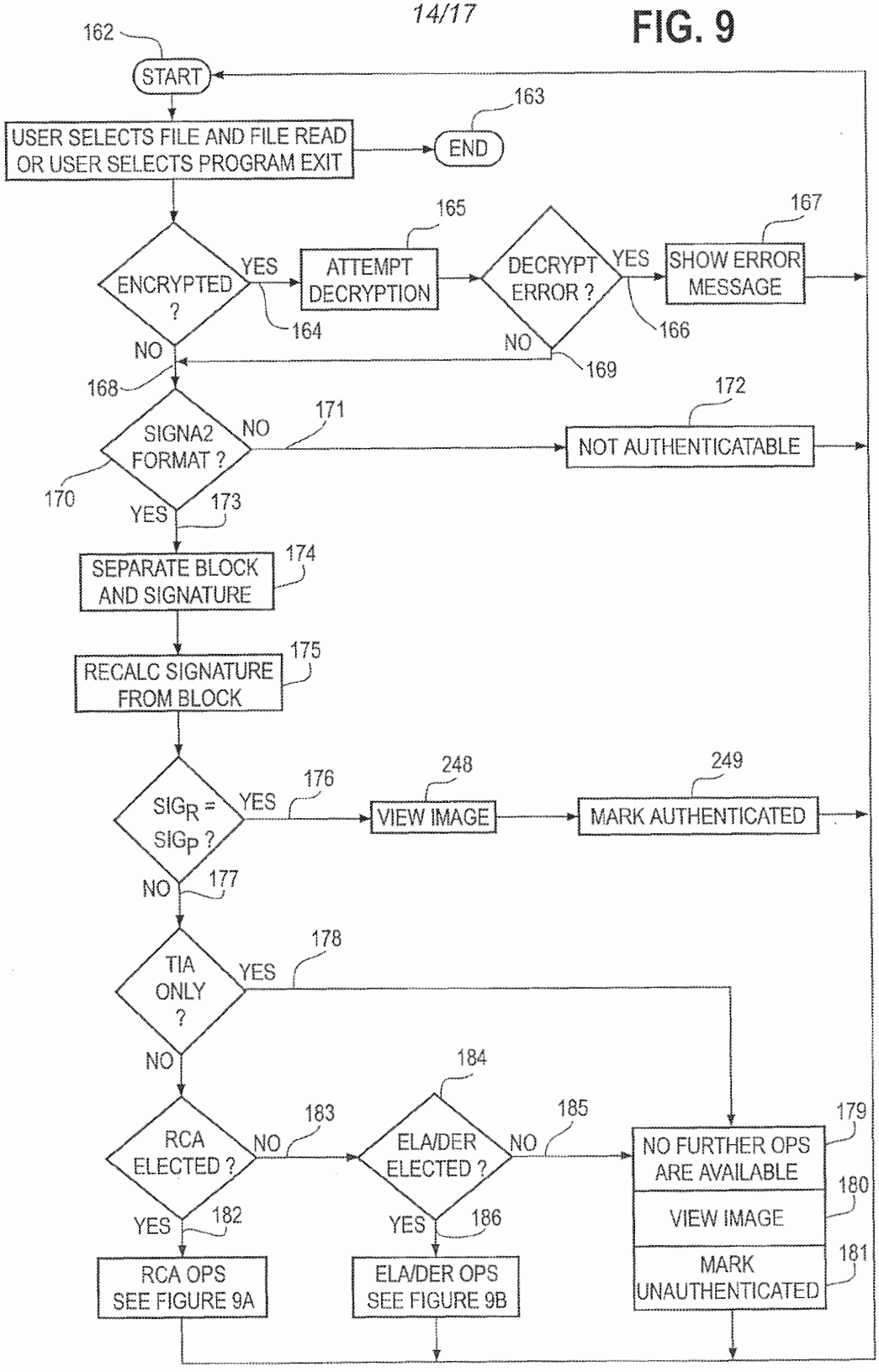

151
DEACTIVATE C-VIBE
152
DEACTIVATE RPY
153
INCREMENT AUTO SEQUENCE NUMBER
NEW RSR ?
YES
154
NO
GENERATE NEW RANDOM STRING
155
RSR SET TO NO
158
RSR USER CONTROL SET TO NO
159
156
DE-ALLOCATE TEMPORARY RESOURCES FOR RE-USE


OIPE JC87
JUL 27 2001
PATENT & TRADEMARK OFFICE


RECEIVED
JUL 31 2001
TC 2100 MAILROOM

14/17

FIG. 9


162
START
USER SELECTS FILE AND FILE READ OR USER SELECTS PROGRAM EXIT
163
END
ENCRYPTED ?
YES
164
ATTEMPT DECRYPTION
165
DECRYPT ERROR ?
YES
166
SHOW ERROR MESSAGE
167
NO
169
NO
168
SIGNA2 FORMAT ?
NO
171
NOT AUTHENTICATABLE
172
170
YES
173
SEPARATE BLOCK AND SIGNATURE
174
RECALC SIGNATURE FROM BLOCK
175
SIGR = SIGP ?
YES
176
VIEW IMAGE
248
MARK AUTHENTICATED
249
NO
177
TIA ONLY ?
YES
178
NO
RCA ELECTED ?
NO
183
ELA/DER ELECTED ?
NO
185
184
NO FURTHER OPS ARE AVAILABLE
VIEW IMAGE
MARK UNAUTHENTICATED
179
180
181
YES
182
RCA OPS SEE FIGURE 9A
YES
186
ELA/DER OPS SEE FIGURE 9B

RECEIVED
JUL 31 2001
TC 2100 MAILROOM



JAFFE-ADO

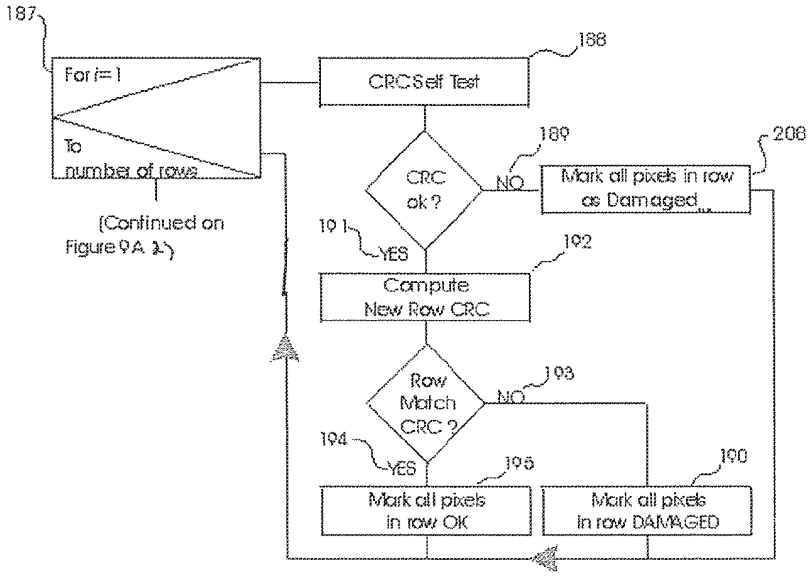

187
For i = 1
To
number of rows
(Continued on
Figure 9A 2)
188
CRC Self Test
189
CRC
ok?
NO
208
Mark all pixels in row
as Damaged
191
YES
192
Compute
New Row CRC
Row
Match
CRC ?
193
NO
194
YES
195
Mark all pixels
in row OK
190
Mark all pixels
in row DAMAGED

FIGURE 9A|

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 16 of 21

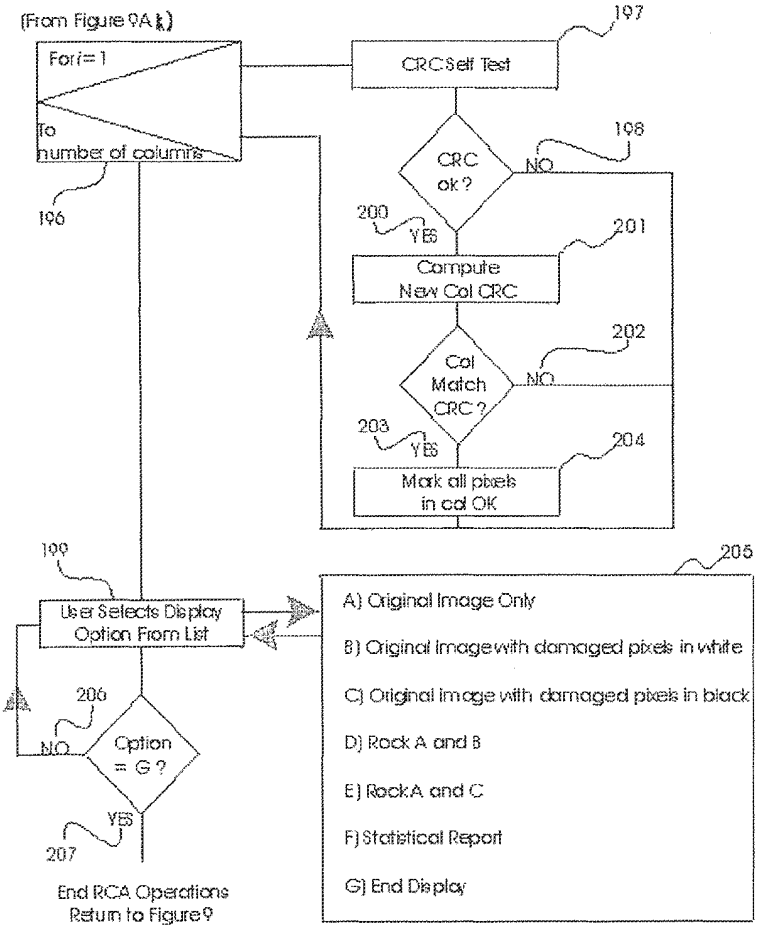
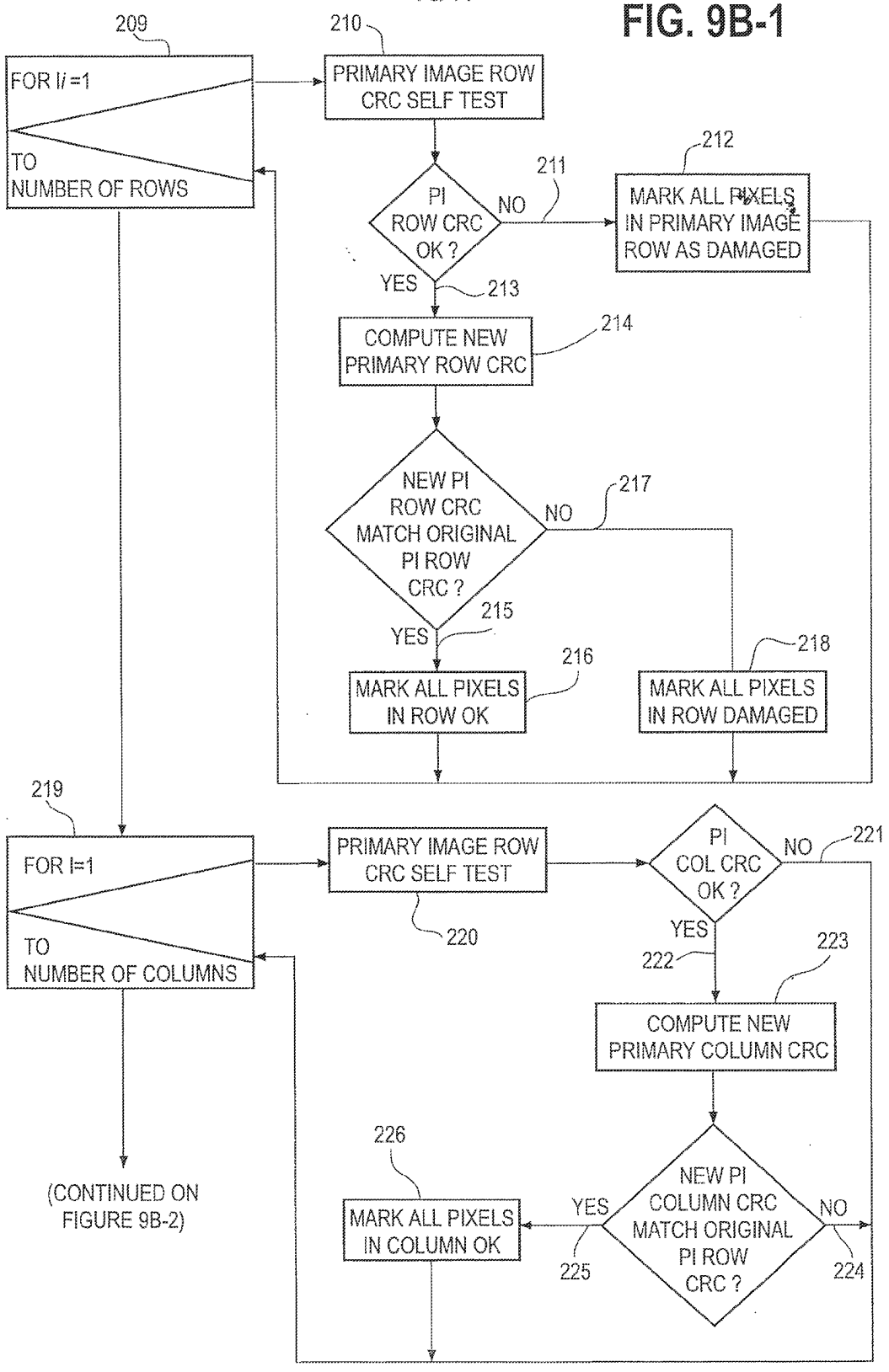

(From Figure 9A1)
For i = 1
to
number of columns
196
CRC Self Test
197
CRC ok ?
198
NO
200
YES
Compute New Col CRC
201
Col Match CRC ?
202
NO
203
YES
Mark all pixels in col OK
204
199
User Selects Display Option From List
205
A) Original Image Only
B) Original image with damaged pixels in white
C) Original image with damaged pixels in black
D) Rock A and B
E) Rock A and C
F) Statistical Report
G) End Display
206
NO
Option = G ?
YES
207
End RCA Operations
Return to Figure 9

FIGURE 9A2

16/17

FIG. 9B-1

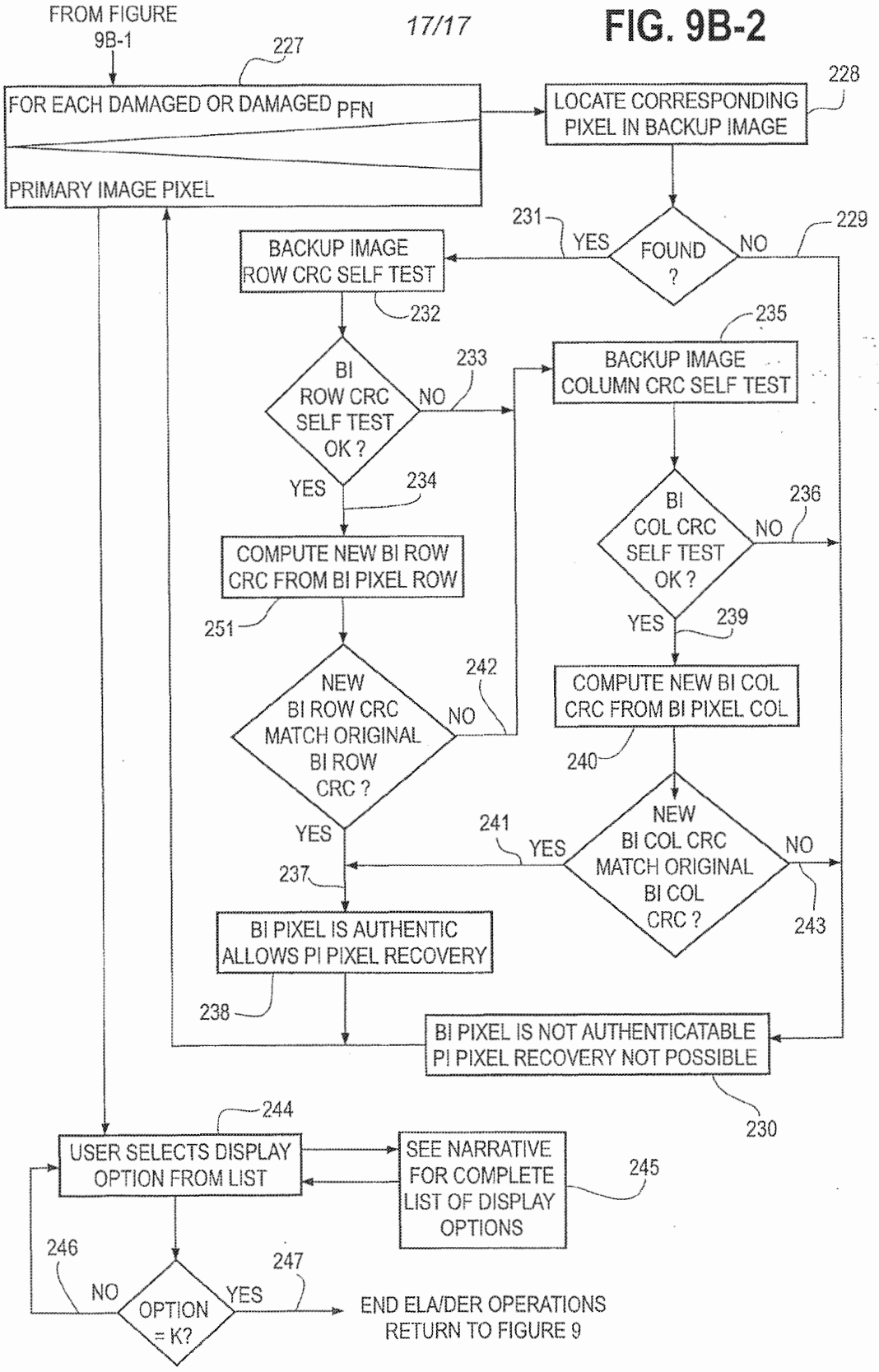

209
FOR I/ =1
TO
NUMBER OF ROWS
210
PRIMARY IMAGE ROW CRC SELF TEST
211
PI ROW CRC OK ?
NO
212
MARK ALL PIXELS IN PRIMARY IMAGE ROW AS DAMAGED
YES
213
214
COMPUTE NEW PRIMARY ROW CRC
NEW PI ROW CRC MATCH ORIGINAL PI ROW CRC ?
217
NO
YES
215
216
MARK ALL PIXELS IN ROW OK
218
MARK ALL PIXELS IN ROW DAMAGED
219
FOR I=1
TO
NUMBER OF COLUMNS
PRIMARY IMAGE ROW CRC SELF TEST
220
PI COL CRC OK ?
NO
221
YES
222
223
COMPUTE NEW PRIMARY COLUMN CRC
226
MARK ALL PIXELS IN COLUMN OK
NEW PI COLUMN CRC MATCH ORIGINAL PI ROW CRC ?
YES
225
NO
224
(CONTINUED ON FIGURE 9B-2)



RECEIVED
JUL 31 2001
TC 2100 MAILROOM

17/17

FIG. 9B-2


FROM FIGURE 9B-1
227
FOR EACH DAMAGED OR DAMAGED PFN
PRIMARY IMAGE PIXEL
228
LOCATE CORRESPONDING PIXEL IN BACKUP IMAGE
231
YES
FOUND ?
NO
229
BACKUP IMAGE ROW CRC SELF TEST
232
BI ROW CRC SELF TEST OK ?
233
NO
YES
234
235
BACKUP IMAGE COLUMN CRC SELF TEST
BI COL CRC SELF TEST OK ?
236
NO
YES
239
COMPUTE NEW BI ROW CRC FROM BI PIXEL ROW
251
COMPUTE NEW BI COL CRC FROM BI PIXEL COL
240
NEW BI ROW CRC MATCH ORIGINAL BI ROW CRC ?
242
NO
YES
NEW BI COL CRC MATCH ORIGINAL BI COL CRC ?
241
YES
NO
243
237
BI PIXEL IS AUTHENTIC ALLOWS PI PIXEL RECOVERY
238
BI PIXEL IS NOT AUTHENTICATABLE PI PIXEL RECOVERY NOT POSSIBLE
230
244
USER SELECTS DISPLAY OPTION FROM LIST
SEE NARRATIVE FOR COMPLETE LIST OF DISPLAY OPTIONS
245
246
NO
OPTION = K?
247
YES
END ELA/DER OPERATIONS RETURN TO FIGURE 9



RECEIVED
JUL 31 2001
TC 2100 MAILROOM

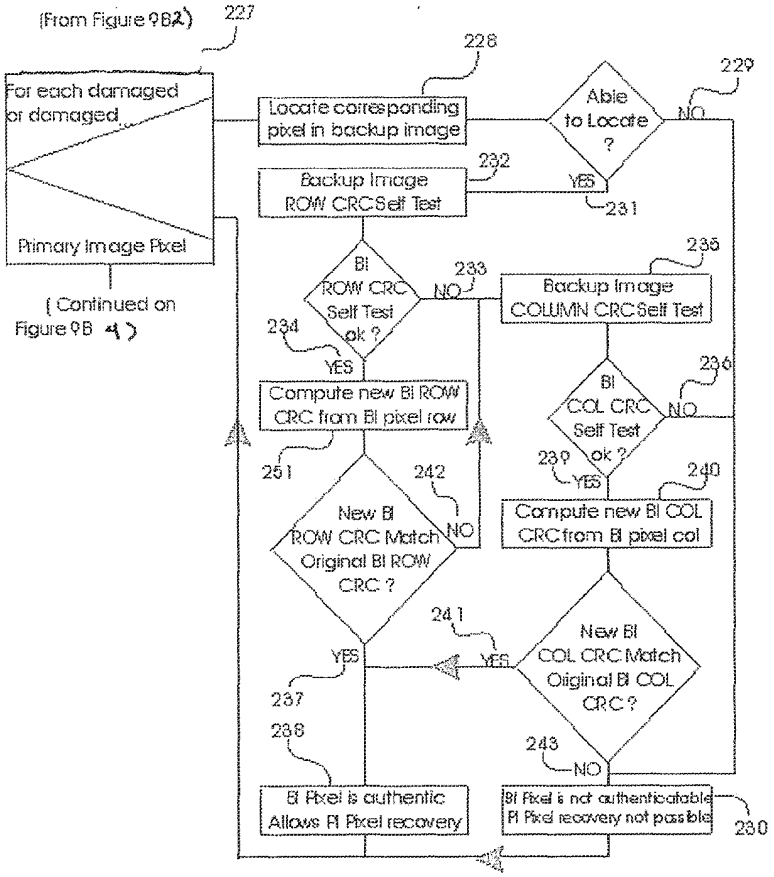

(From Figure 9B2)
227
For each damaged or damaged
Primary Image Pixel
(Continued on Figure 9B 4)
228
Locate corresponding pixel in backup image
229
Able to Locate ?
NO
YES
231
232
Backup Image ROW CRC Self Test
BI ROW CRC Self Test ok ?
233
NO
234
YES
235
Backup Image COLUMN CRC Self Test
BI COL CRC Self Test ok ?
236
NO
239
YES
240
Compute new BI COL CRC from BI pixel col
Compute new BI ROW CRC from BI pixel row
251
242
New BI ROW CRC Match Original BI ROW CRC ?
NO
241
YES
New BI COL CRC Match Original BI COL CRC ?
243
NO
YES
237
238
BI Pixel is authentic Allows PI Pixel recovery
BI Pixel is not authenticatable PI Pixel recovery not possible
230

FIGURE 9B3

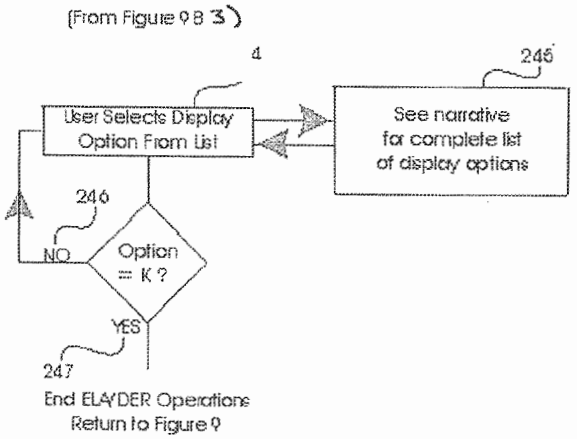

(From Figure 9B 3)
4
246
User Selects Display Option From List
See narrative for complete list of display options
246
NO
Option = K ?
YES
247
End ELAYDER Operations Return to Figure 9

FIGURE 9B4

Applicant(s): Jonathan E. Jaffe et al.
for: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**
Atty. Docket No. 6468/78445
Welsh & Katz, Ltd.
(312) 655-1500
Sheet 21 of 21

Office Action Summary	Application No.	Applicant(s)	
	09/626,044	JAFFE ET AL.	
	Examiner	Art Unit	
	Hosuk Song	2131	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

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

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-8 are rejected under 35 U.S.C. 102(b) as being anticipated by Schipper et al.(US 5,764,770).

Claim 1: Schipper disclose an apparatus for allowing a data stream to be authenticated comprising a memory in (col.7,lines 62-67 and col.8,lines 1-15). Schipper disclose a circuit that is adapted to store a data stream in memory in which the circuit allowing to be determined whether or not the data stream has been altered after it has been stored in the memory in (col.14,lines 42-65). Schipper disclose storing at least one parameter in the memory with the data string, at least one parameter being generally representative of at least one condition under which data stream was generated in (col.15,lines 30-45,59-67). Schipper disclose utilizing data stream and parameter to generate a first signature that is stored in the memory with the data stream and generating a second signature from the data stream and stored at least one parameter in (col.22,lines 27-49). Schipper disclose comparing two signatures in (col.25,lines 36-51).

Claim 2: Schipper disclose circuit and memory form a part of a digital camera in (fig.7 and col.59-67).

Claim 3: Schipper disclose GPS coordinate in (fig.1,6).

Claim 4: Schipper disclose data stream is a digital sample of an environment in (col.7,lines 63-67 and col.8,lines 2-15).

Claim 5: Schipper disclose storing a data stream in a memory in (col.7,lines 63-67). Schipper disclose storing at least one parameter in memory at least one parameter being

generally representative of at least one condition under which data stream was generated in (col.8,lines 8-15). Schipper disclose utilizing data stream and at least one parameter to generate a first signature that is stored in the memory with data stream in (col.8,lines 34-44). Schipper disclose generating a second signature from the data stream and parameters at a point in time subsequent to computation of the first signature in (col.22,lines 27-49). Schipper disclose comparing two signatures in (col.25,lines 36-51).

Claim 6: Schipper disclose circuit and memory form a part of a digital camera in (fig.7 and col.59-67).

Claim 7: Schipper disclose data stream is a digital sample of an environment in (col.7,lines 63-67 and col.8,lines 2-15).

Claim 8: Schipper disclose GPS coordinate in (fig.1,6).

Conclusion

2. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Friedman (US 5,499,294) disclose a digital camera with a processor for authentication of images produced from an image file taken by the digital camera.

b. Schumacher et al.(US 6,269,446) disclose image authentication from digital camera with GPS derived time and location.

c. Ellis et al.(US 5,504,518) disclose digital signature method for broadcast video signal.

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hosuk Song whose telephone number is 703-305-0042. The examiner can normally be reached on Tue-Fri from 6:00 am – 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

HSS
August 12, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Notice of References Cited	Application/Control No. 09/626,044	Applicant(s)/Patent Under Reexamination JAFFE ET AL.	
	Examiner Hosuk Song	Art Unit 2135	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6269446	7-2001	SCHUMACHER ET AL.	713/176
	B	US-5504518	04-1996	ELLIS ET AL.	725/22
	C	US-5764770	06-1998	SCHIPPER ET AL.	713/176
	D	US-5499294	03-1996	FRIEDMAN	713/179
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

US006269446B1

(12) **United States Patent**
Schumacher et al.

(10) **Patent No.: US 6,269,446 B1**
(45) **Date of Patent: Jul. 31, 2001**

(54) **AUTHENTICATING IMAGES FROM DIGITAL CAMERAS**

(75) Inventors: **Thomas Schumacher**, Cupertino; **Timothy L. Kohler**, San Jose, both of CA (US)

(73) Assignee: **Canon Kabushiki Kaisha**, Tokyo (JP)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/105,046**

(22) Filed: **Jun. 26, 1998**

(51) **Int. Cl.**[7] **H04L 9/32**; H04L 9/30

(52) **U.S. Cl.** **713/176**; 713/179; 713/181; 380/30

(58) **Field of Search** 713/160, 161, 713/162, 176, 177, 178, 179, 181; 380/30, 179, 234, 279

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,005,200		4/1991	Fischer	380/30
5,027,401		6/1991	Soltesz	380/54
5,499,294		3/1996	Friedman	380/10
5,579,393	*	11/1996	Conner et al.	380/25
5,629,981		5/1997	Nerlikar	380/25
5,659,617		8/1997	Fischer	380/25
5,712,914		1/1998	Aucsmith et al.	380/30
5,787,172	*	7/1998	Arnold	380/21
5,799,083		8/1998	Brothers et al.	380/20
6,105,134	*	8/2000	Pinder et al.	713/170
6,111,953	*	8/2000	Walker et al.	380/51

OTHER PUBLICATIONS

"Introduction to Message Privacy", <http:/www/pgp.com/privacy/intro–priv.cgi#mpriv–digsigs>, 6 pages, (visited Dec. 17, 1997).

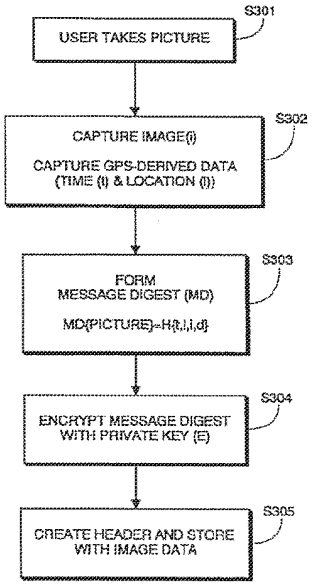
* cited by examiner

Primary Examiner—Tod Swann
Assistant Examiner—Justin T. Darrow
(74) *Attorney, Agent, or Firm*—Fitzpatrick, Cella, Harper & Scinto

(57) **ABSTRACT**

Authentication of image from digital cameras with GPS-derived time and location data is disclosed. With the widespread availability of today's desktop tools and imaging devices, unethical manipulation of digital image data is common, such that digital images are not ordinarily reliable and can be subject to trickery and forgery. In the past, imagery such as photographs and digital images were reliable enough to serve as documentary evidence in most cases, since a skilled craftsman was needed to modify the images and commit fraud. However, skilled craftsmen are no longer needed, and digital images can be modified by even a casual user. Moreover, time data and location data are not ordinarily included in digital images. According to the invention, a digital camera system documents the time, date and location where a digital image was taken, using GPS-derived data from a secure connection. The validity and authenticity of the digital image, as well as the time data and location data, is then protected with a public key signature system that provides a digital signature by which the image and time and location information can be authenticated.

59 Claims, 4 Drawing Sheets



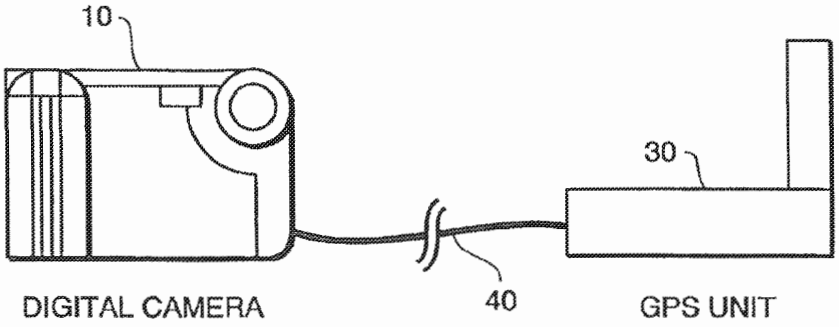

10
30
DIGITAL CAMERA
40
GPS UNIT

FIG. 1

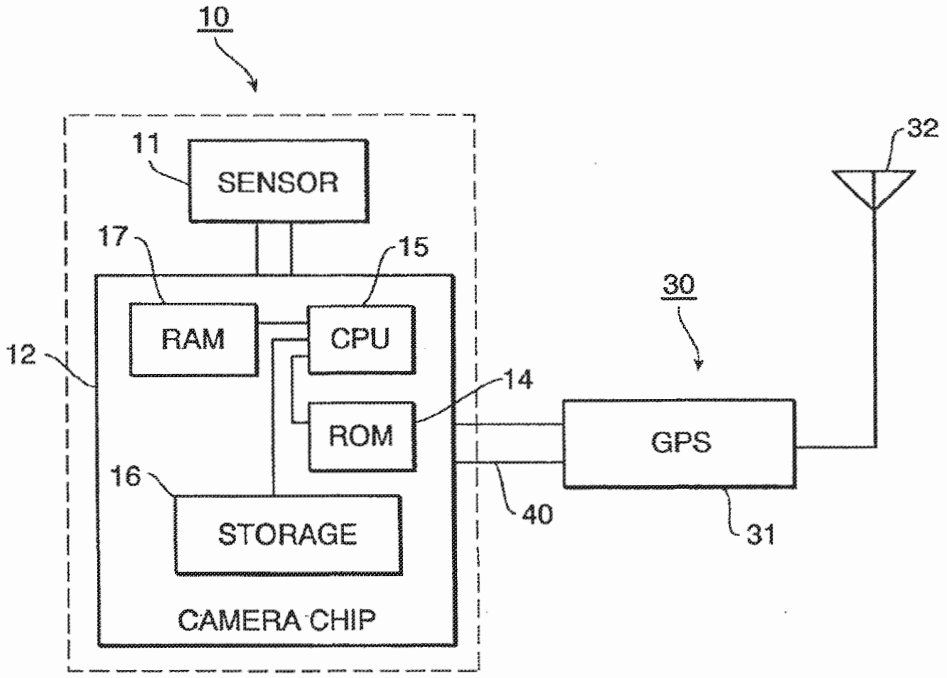

10
11
SENSOR
17
15
RAM
CPU
12
14
ROM
16
STORAGE
CAMERA CHIP
30
GPS
32
40
31

FIG. 2

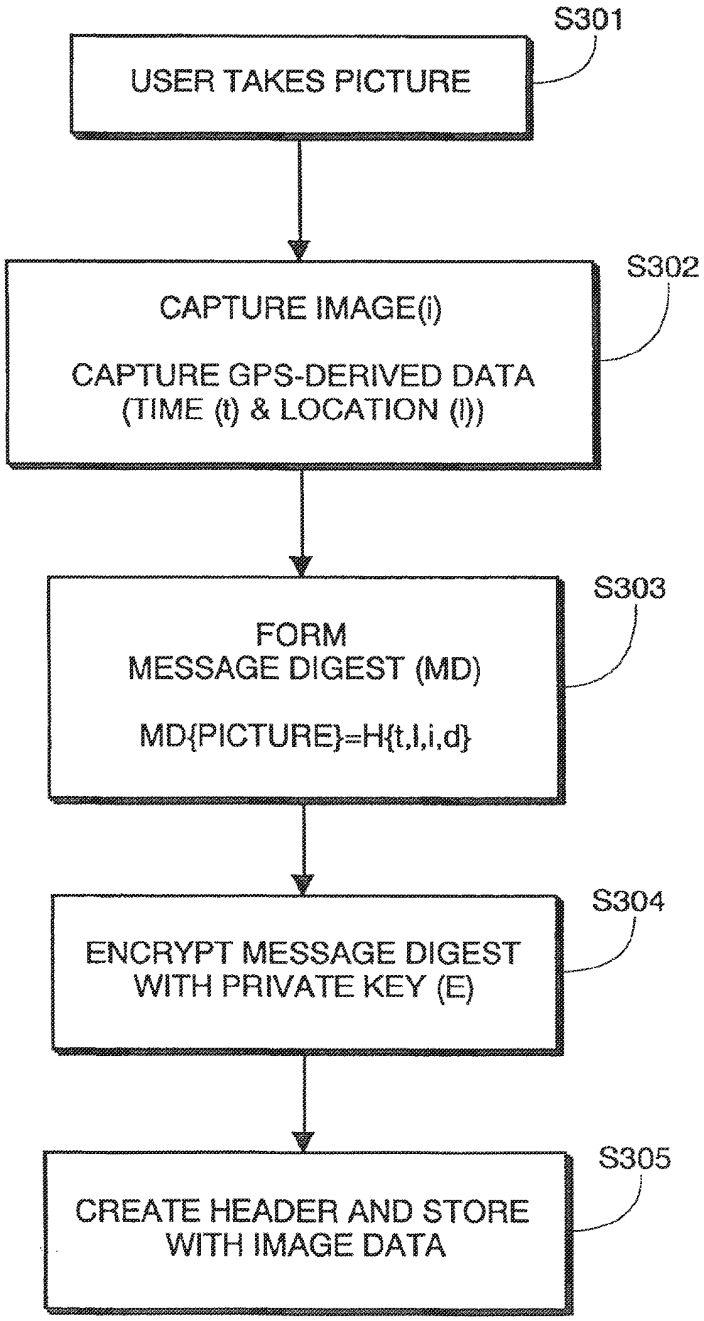

S301
USER TAKES PICTURE
S302
CAPTURE IMAGE(i)
CAPTURE GPS-DERIVED DATA
(TIME (t) & LOCATION (l))
S303
FORM
MESSAGE DIGEST (MD)
MD{PICTURE}=H{t,l,i,d}
S304
ENCRYPT MESSAGE DIGEST
WITH PRIVATE KEY (E)
S305
CREATE HEADER AND STORE
WITH IMAGE DATA

FIG. 3

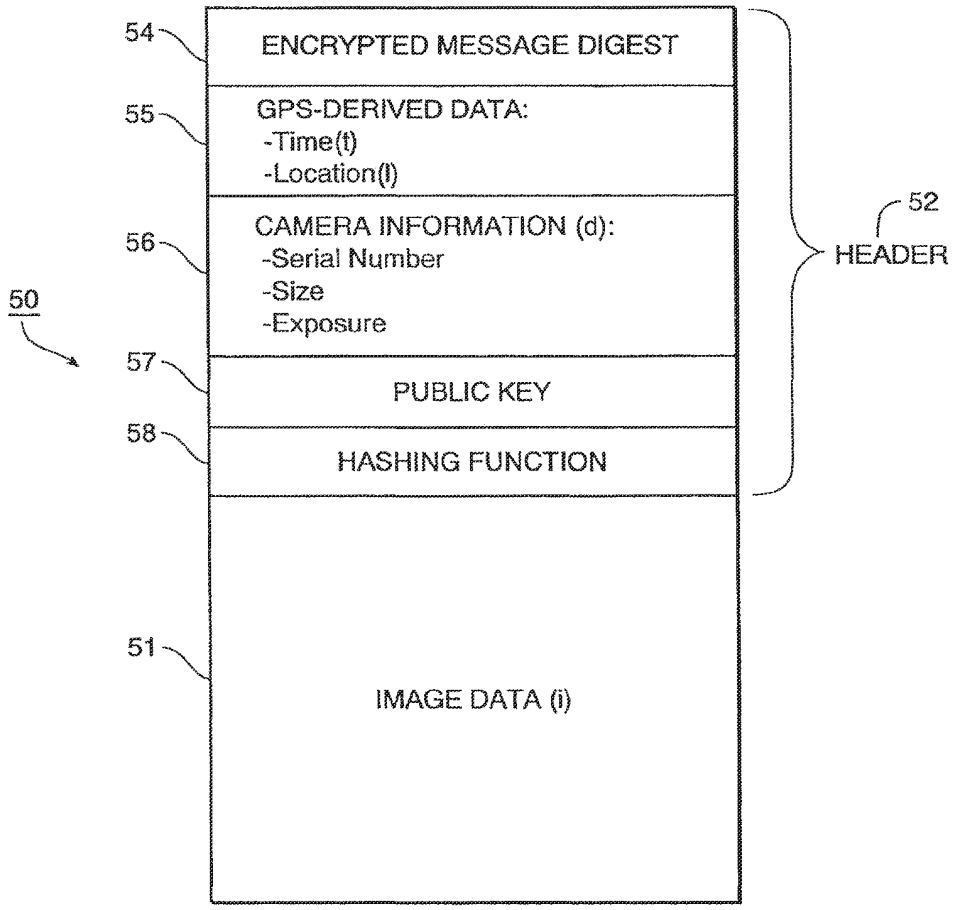

54
ENCRYPTED MESSAGE DIGEST
55
GPS-DERIVED DATA:
-Time(t)
-Location(l)
56
CAMERA INFORMATION (d):
-Serial Number
-Size
-Exposure
57
PUBLIC KEY
58
HASHING FUNCTION
52
HEADER
50
51
IMAGE DATA (i)

FIG. 4

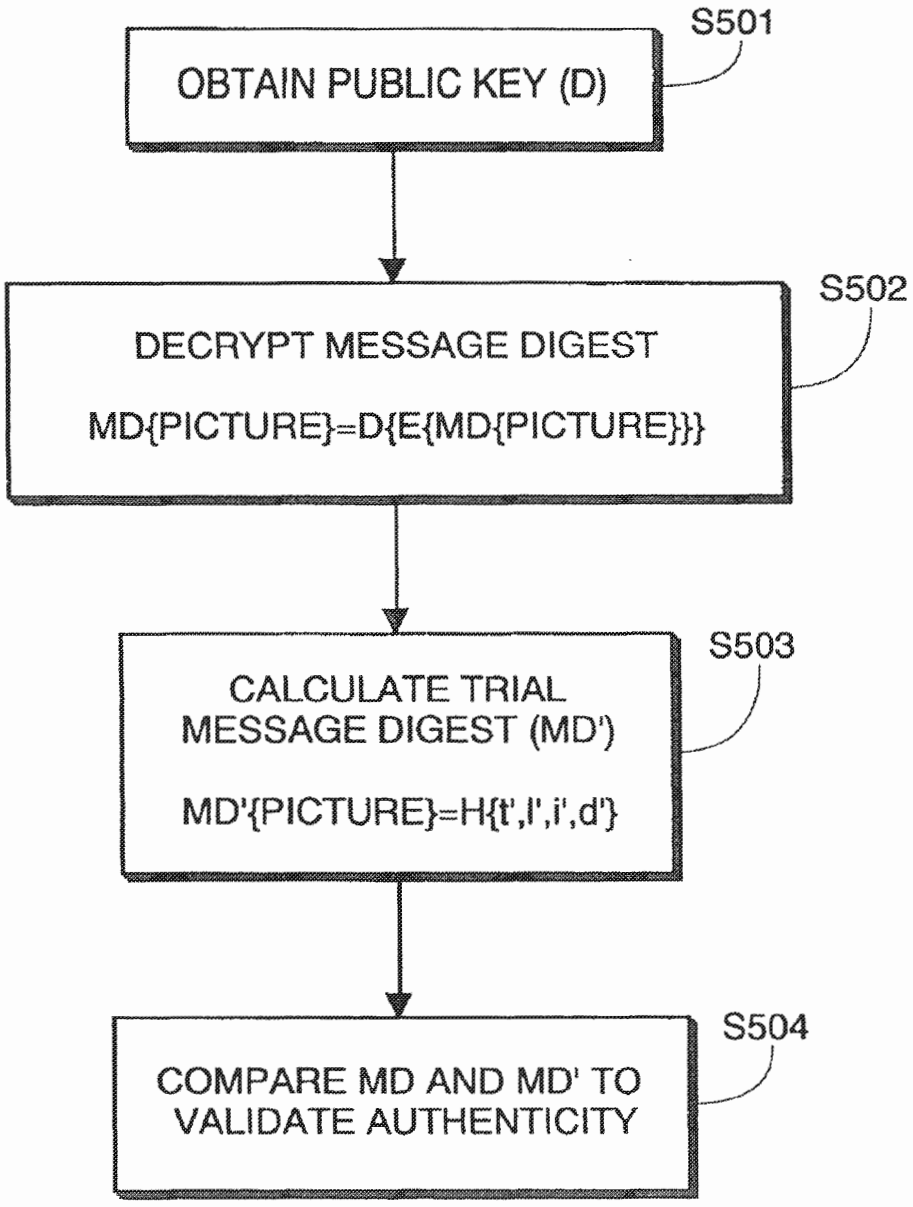

S501
OBTAIN PUBLIC KEY (D)
S502
DECRYPT MESSAGE DIGEST
MD{PICTURE}=D{E{MD{PICTURE}}}
S503
CALCULATE TRIAL MESSAGE DIGEST (MD')
MD'{PICTURE}=H{t',l',i',d'}
S504
COMPARE MD AND MD' TO VALIDATE AUTHENTICITY

FIG. 5

AUTHENTICATING IMAGES FROM DIGITAL CAMERAS

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to public key/private key authentication of images from digital cameras, and more particularly relates to public key/private key authentication of images from digital cameras with global positioning system (GPS) data.

2. Description of the Related Art

Digital cameras have become popular devices for producing high quality digital images of photographic scenes. In general, digital cameras create a digital image by exposure of a CCD sensor array to a photographic scene, followed by conversion of the CCD data to digital image data that is stored in the camera. Thereafter, the digital image data stored in the camera may be transferred to a personal computer or other more permanent storage for printout, viewing, transmission and the like.

One problem with digital image data, however, is the ease with which such data can be manipulated or changed, thereby creating a false representation of the original photographic scene. Such problems are particularly prevalent in certain fields such as forensics and legal or law enforcement fields, where it is essential to prove the authenticity of images. Because of the ease with which digital images may be altered so as to distort the appearance of the original photographic scene, proof of authenticity can often be difficult and sometimes impossible.

Conventional approaches to proving authenticity of digital images have involved the use of public key/private key digital signatures. One such conventional approach is described in U.S. Pat. No. 5,499,294 to Friedman. Friedman's approach involves the use of an embedded private key in a digital camera, with the private key being used to create a digital signature based on a message digest of the image data. Thereafter, a user wishing to authenticate the image data obtains a public key that corresponds to the embedded private key. As is known in conventional public key/private key authentication, the public key and the private key correspond to each other such that only one public key can decrypt data encrypted with the private key, and vice-versa. Accordingly, through use of the public key, a user of Friedman's system is able to authenticate that image data has not been modified since when it was originally obtained by the digital camera.

One drawback of the Friedman system is its inability also to provide authentication of the photographic event, such as authentication of the time, date and position of the photographic scene involved, at least without visually distorting the digital image of the photographic scene. Specifically, Friedmin's system contemplates an arrangement in which GPS-derived position information is inserted as image data in a frame surrounding the photographic scene. However, such a frame detracts from the visual appearance of the image, making the image less pleasing to the viewer. Moreover, use of such data to authenticate the event is entirely manual, since the data is visual and must be inspected by a human operation. In addition, since the GPS-derived data is actually stored as image data, it is difficult to use the GPS-derived data for other purposes, such as sorting or cataloging.

SUMMARY OF INVENTION

It is therefore an object of the invention to authenticate events and images from digital cameras with GPS-derived data, by deriving a digital signature based on both coded GPS data and the image data, and by storing the digital signature in a header for a file with the image data.

Thus, in one aspect, the invention authenticates image data from digital cameras that have captured GPS-derived data as well as image data. A message digest is created for the image data, with the message digest being derived from the image data itself together with GPS-derived data such as time stamp data, location data. It is also preferable to include camera information data, such as serial number of the camera, size information, exposure information, and the like. The message digest is encrypted with a private key secure with the digital camera, and an image file is created together with a header that includes the private-key-encrypted message digest together with the unencrypted data that went into forming the message digest. For convenience, other information may also be stored in the header, such as a public key used to decrypt the encrypted message digest and which corresponds to the private key, and such as an identifier for the hashing function used to create the message digest.

The encrypted message digest forms a digital signature which verifies the authenticity of the image data, and which also verifies the authenticity of the event based on the GPS-derived data in the header. Moreover, because the GPS-derived data is stored in a header and not as part of the image data, the GPS-derived data can be used for other purposes such as sorting and cataloging, and the visual appearance of the image data is not distorted by the presence of unwanted GPS data.

In other aspects, the invention is verification of the authenticity of digital camera images having GPS-derived data. According to this aspect, to verify the authenticity of digital camera images, a public key is obtained, for example, from a trusted party. The public key is used to decrypt the private-key-encrypted message digest, so as to obtain a message digest for the picture. A trial message digest is calculated, using the same hashing function as was used by the digital camera to form the original message digest. The trial message digest is compared to the decrypted message digest for equality. If the two message digests agree, then the image data and the GPS-derived data are authenticated; conversely, if the two message digests do not agree, the image data and the GPS data cannot be trusted.

A additional feature of the invention involves the provision of a secure connection between a GPS receiver and a digital camera. Specifically, as can be appreciated from the foregoing explanation, one potentially weak link in the authentication/verification sequence is the connection between GPS information and the digital camera. If such a link is not secure, then it is possible for GPS data to be simulated to the digital camera, thereby resulting in forged images from the digital camera. To combat this possibility, a secure connection is provided between the GPS receiver and the digital camera, with the secured connection taking the form of either a public is key/private key encryption arrangement between the GPS receiver and the digital camera, or alternatively a GPS receiver that is built into the camera or resides on the same integrated circuit as the camera.

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

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a perspective view of the outward appearance of an embodiment of the invention.

FIG. **2** is a block diagram of the FIG. **1** embodiment.

FIG. **3** in a flow diagram for explaining how a digital signature is derived for image data.

FIG. **4** is a view for explaining the format of an image file including a header that contains an authenticated digital signature.

FIG. **5** is a flow diagram for explaining how to verify the authenticity of image data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** is a view of the outward appearance of an embodiment of the present invention, in which a digital signature is obtained for image data from a digital camera. Specifically, shown in FIG. **1** is a digital camera **10** connected to a GPS unit **30** over a secure connection **40**. Digital camera **10** obtains a digital image for a photographic scene by exposing a CCD sensor array to the photographic scene and converting the CCD data into digital data. GPS unit **30** obtains GPS-derived data such as time and location data through conventional triangulation techniques using the GPS grid of orbital satellites. Although the presently-described embodiment illustrates use of GPS unit **30** so as to derive time and location data, the practice of the invention is not limited to a GPS receiver for providing such information, and any now-known or future-developed system for providing time and location data over a secure link to digital camera **10** may also be used in the practice of the invention.

Secure link **40** provides a secure connection between digital camera **10** and GPS unit **30**, thereby preventing a forger from masquerading himself as GPS unit **30** and providing false time and location information to digital camera **10**, specifically, secure link **40** may comprise a public key/private key authentication arrangement between GPS unit **30** and digital camera **10**, such that the time and location information from GPS unit **30** includes a digital signature encrypted by a private key known only to GPS unit **30**. Digital camera **10**, upon receipt of time and location information from GPS unit **30**, uses a public key from a trusted source so as to validate the authenticity of the digital signature, before permitting use of the time and location information from the secure link.

Alternatively, although FIG. **1** depicts digital camera **10** as a unit separate from GPS unit **30**, it is possible to provide a secure link by incorporating a GPS receiver into digital camera **10** itself, or more preferably on the same chip as the digital camera.

FIG. **2** depicts a block diagram of the FIG. **1** embodiment. As shown in FIG. **2**, digital camera **10** includes a sensor array **11** of CCD sensors which are exposed to a photographic scene through an unshown lens and exposure control mechanism. Digital camera **10** further includes a camera chip **12** on which are arranged a ROM **14** for storing program instruction sequences that control the digital camera, together with a CPU **15** which executes the program instruction sequences so as to cause the digital camera to expose sensor array **11** to a photographic scene and derive digital image data corresponding to the photographic scene. The digital image data is stored in memory storage section **16**. The memory storage section **16** may be removable, so as to facilitate transfer of the digital image data to other devices such as a PC, and/or camera **10** may be provided with an unshown interface so as to facilitate transfer of digital image data even if memory storage **16** is not removable. A RAM **17** is further provided so as to provide camera **10** with short term and scratch pad random access memory, particularly for use in deriving a digital signature for the digital image.

GPS **30** includes a GPS receiver **31** and a GPS antenna **32**, and is connected to camera **10** over secure connection **40**.

FIG. **3** is a flow diagram explaining process steps stored in a memory medium such as ROM **14**, by which digital image data obtained by camera **10** is provided with a digital signature that can be used to authenticate the validity of the image data together with the validity of event time and location information stored with the image. Briefly, according to FIG. **3**, based on image information and event information from the GPS-derived information captured by camera **10**, a message digest is formed by a hashing function that utilizes both the image data and the GPS-derived data. The message digest is encrypted with a private key known only to camera **10**, thereby forming a digital signature which can be used to validate the authenticity of the image data as well as the authenticity of the GPS-derived data. Thereafter, the digital image is stored in memory storage **16** together with a header that includes the encrypted message digest, as well as unencrypted GPS-derived data.

In more detail, upon a user's taking of a picture in step S**301**, digital camera 1o captures image data from sensor **11**, and further captures GPS-derived data including time and location data from GPS unit **30** over secure link **40** (in step S**302**). Step S**303** calculates a message digest for the image data and for the GPS-derived data. The message digest is calculated using a hashing function which, through prearrangement, is the same hashing function that is used to validate the authenticity of the image. The purpose of the hashing function is to derive a short digest of the image information and the GPS-derived data, with the property that even if a single bit of such information is changed, a different digest would result In this embodiment of the invention, a message digest MD for the image is derived from a hashing function H as follows:

$$MD\{\text{picture}\}=H\{t+l+i+d\}$$

where t is time information and 1 is location information, both derived from the GPS, i is the digital image data itself, and d is camera information such as serial number, size and exposure information.

Thereafter, in step S**304**, digital camera **10** encrypts the message digest with a private key E. Specifically, camera **10** has associated with it a unique private key not known outside of camera **10**. One possibility is to store the private key B in ROM **14**, although other and more tamper-free arrangements may be provided. The private key has a complementary public key which operates such that only the public key can decrypt information encrypted by the private key, and vice-versa (i.e., only the private key can decrypt information encrypted by the public key).

In step S**305**, digital camera **10** stores the image data in storage section **16**, with the image data being stored in a file together with header information that includes the encrypted message digest, as well as unencrypted information that went into the message digest. In this embodiment of the invention, since time and location data from the GPS-derived data, as well as camera information are all included in the message digest, the header includes the time and location information as well as the camera information.

FIG. **4** illustrates one preferable format for the image file. As shown in FIG. **4**, image file **50** includes digital image

data i at section **51**, and further includes header information **52**. The header information includes the encrypted message digest **54**, the GPS-derived data **55** including time data (t) and location data (l) and camera information **56** (d) including camera serial number, size and exposure information. As a convenience, header **52** may als include a public key **57** and the identity of the hashing function **58**; however, these are more preferably obtained from a more trusted source, such as a centralized source of public information, so as to prevent forgeries simply through use of incorrect public keys or hashing functions. Thus, providing public key **57** and the identify **58** of the hashing function within the header is a matter of convenience only.

FIG. **5** is a flow diagram illustrating process steps on a memory medium such as ROM **14** or on disk in a personal computer (PC), by which the authenticity of image data and event data (time and location data) are verified. The process steps shown in FIG. **5** may be carried out in camera **10**, but more preferably they are carried out in another device such as a personal computer that has access to file so (such as through transfer of such files from storage section **16**) and desires to confirm the authenticity of the file.

Briefly, according to FIG. **5**, to validate the authenticity of a digital image that contains a digital signature for image data and for GPS-derived event data, a public key is obtained such as from a trusted party, and is used to decrypt the digital signature so as to obtain a decrypted message digest. Then, a trial message digest is calculated using a previously agreed-upon hashing function, and based on the image data in the image file and the unencrypted time and location data in a header for the image file The trial message digest is compared against the decrypted message digest, and if the two message digests agree then the image data is validated as authentic; conversely, if the two message digests do not agree, then the image data cannot be trusted.

In more detail, step **S501** obtains the public key D that complements the private key E used by digital camera **10**. The public key is preferably obtained from a trusted source such as publicly available information that publishes public keys in correspondence to serial numbers of cameras. Alternatively, the public key D can be obtained from header **52** of the image file, although this source is less trustworthy since it can be forged.

Step **S502** uses the public key D to decrypt the encrypted message digest **54**. The decrypted message digest MD thus represents a decryption of the digital signature:

$$MD\{\text{picture}\}=D\{E\{KD\{\text{picture}\}\}\}$$

Step **S503** calculates a trial message digest MD'. The trial message digest is calculated with the same hashing as was used by digital camera **10**, either through pre-arrangement or by obtaining the identity of the hashing function from field **58** of header **52**. The trial message digest is calculated using the same information used by digital camera **10** to create the original message digest, and uses the unencrypted information stored in header **52**. Thus, in this embodiment of the invention, the trial message digest is based on the unencrypted codes for GPS-derived time and location information, as well as the image information itself and camera information such as serial number, size and exposure:

$$MD'\{\text{picture}\}=H\{t'+l'+i'+d'\}$$

where primes (e.g., "t" are used to denote corresponding information obtained from the file header.

Step **S504** compares the trial message digest MD' to the decrypted message digest MD. If the two message digests are the same, then the authenticity of both the image data and the GPS-derived data is validated. Conversely, if the two message digests do not agree, the image data cannot be trusted.

While the invention is described above with respect to what is currently considered its preferred embodiments, it is to be understood that the invention is not limited to that described above. To the contrary, the invention is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

What is claimed is:

1. A method for forming a digital signature for authentication of image data for a digital camera that has captured event data for the image data, comprising the steps of:

creating a message digest for the image data, the message digest being derived from the image data and from the event data;

encrypting the message digest with a private key unique to and secured with the digital camera; and

creating an image file for the image data, the image file having a header that includes the private-key-encrypted message digest together with unencrypted event data.

2. A method according to claim **1**, wherein the event data comprises GPS-derived data.

3. A method according to claim **1**, wherein the event data includes time stamp data and location data.

4. A method according to claim **3**, wherein said step of creating the message digest includes creating the message digest with digital camera information data.

5. A method according to claim **3**, wherein said header includes unencrypted camera information data.

6. A method according to claim **1**, wherein said header includes a public key complementary to the private key and which can be used to decrypt the encrypted message digest.

7. A method according to claim **1**, wherein said step of creating a message digest includes the step of using a hashing function which through pre-arrangement can be used to validate authenticity based on unencrypted data in the header.

8. A method according to claim **7**, wherein said header includes an identifier for the hashing function.

9. An apparatus for forming a digital signature for authentication of image data for a digital camera that has captured event data for the image data, said apparatus comprising:

a first creation means for creating a message digest for the image data, the message digest being derived from the image data and from the event data;

means for encrypting the message digest with a private key unique to and secured with the digital camera; and

a second creation means for creating an image file for the image data, the image file having a header that includes the private-key-encrypted message digest together with unencrypted event data.

10. An apparatus according to claim **9**, wherein the event data comprises GPS-derived data.

11. An apparatus according to claim **9**, wherein the event data includes time stamp data and location data.

12. An apparatus according to claim **11**, wherein said first creation means includes means for creating the message digest with digital camera information data.

13. An apparatus according to claim **11**, wherein said header includes unencrypted camera information data.

14. An apparatus according to claim **9**, wherein said header includes a public key complementary to the private key and which can be used to decrypt the encrypted message digest.

15. An apparatus according to claim 9, wherein said first creation means includes a hashing function which through pre-arrangement can be used to validate authenticity based on unencrypted data in the header.

16. An apparatus according to claim 15, wherein said header includes an identifier for the hashing function.

17. An apparatus for forming a digital signature for authentication of image data for a digital camera that has captured event data for the image data, comprising:

a program memory for storing process steps of: (1) creating a message digest for the image data, the message digest being derived from the image data and from the event data, (2) encrypting the message digest with a private key unique to and secured with the digital camera, and (3) creating an image file for the image data, the image file having a header that includes the private-key-encrypted message digest together with unencrypted event data; and

a processor for executing the process steps stored in said memory.

18. An apparatus according to claim 17, wherein the event data comprises GPS-derived data.

19. An apparatus according to claim 17, wherein the event data includes time stamp data and location data.

20. An apparatus according to claim 19, wherein said step of creating the message digest includes creating the message digest with digital camera information data.

21. An apparatus according to claim 19, wherein said header includes unencrypted camera information data.

22. An apparatus according to claim 17, wherein said header includes a public key complementary to the private key and which can be used to decrypt the encrypted message digest.

23. An apparatus according to claim 17, wherein said step of creating a message digest includes the step of using a hashing function which through pre-arrangement can be used to validate authenticity based on unencrypted data in the header.

24. An apparatus according to claim 23, wherein said header includes an identifier for the hashing function.

25. Computer-executable process steps stored on a computer readable medium, said computer-executable process steps for forming a digital signature for authentication of image data for a digital camera that has captured event data for the image data, said computer-executable process steps comprising:

a first creating step to create a message digest for the image data, the message digest being derived from the image data and from the event data;

an encrypting step to encrypt the message digest with a private key unique to and secured with the digital camera; and

a second creating step to create an image file for the image data, the image file having a header that includes the private-key-encrypted message digest together with unencrypted event data.

26. Computer-executable process steps according to claim 25, wherein the event data comprises GPS-derived data.

27. Computer-executable process steps according to claim 25, wherein the event data includes time stamp data and location data.

28. Computer-executable process steps according to claim 27, wherein said first creating step to create a message digest includes a creating step to create the message digest with digital camera information data.

29. Computer-executable process steps according to claim 27, wherein said header includes unencrypted camera information data.

30. Computer-executable process steps according to claim 25, wherein said header includes a public key complementary to the private key and which can be used to decrypt the encrypted message digest.

31. Computer-executable process steps according to claim 25, wherein said first step of creating to create a message digest includes a using step to use a hashing function which through pre-arrangement can be used to validate authenticity based on unencrypted data in the header.

32. Computer-executable process steps according to claim 31, wherein said header includes an identifier for the hashing function.

33. A method for validating authenticity of an image file containing image data and a header that includes a private-key-encrypted message digest together with unencrypted data including event data that went into forming the message digest, said method comprising the steps of:

obtaining a public key complementary to a private key used to encrypt the message digest;

decrypting the private-key-encrypted message digest using the public key so as to obtain a message digest;

calculating a trial message digest using a hashing function the same as the hashing function used to form the private-key-encrypted message digest, and also using the unencrypted event data in the header; and

comparing the trial message digest to the decrypted message digest to determine the authenticity of the image file,

wherein the event data includes location data.

34. A method according to claim 33, wherein the location data comprises GPS-derived data.

35. A method according to claim 33, wherein said step of obtaining the public key comprises the step of obtaining the public key from a trusted party.

36. A method according to claim 33, wherein said step of obtaining the public key comprises the step of obtaining the public key from the header.

37. A method according to claim 33, wherein said header includes camera information, and wherein said step of calculating a trial message digest comprises a step of calculating the trial message digest using the camera information.

38. A method according to claim 37, further comprising the step of obtaining an identity of the hashing function from the header.

39. An apparatus for validating authenticity of an image file containing image data and a header that includes a private-key-encrypted message digest together with unencrypted data including event data that went into forming the message digest, said apparatus comprising:

means for obtaining a public key complementary to a private key used to encrypt the message digest;

means for decrypting the private-key-encrypted message digest using the public key so as to obtain a message digest;

means for calculating a trial message digest using a hashing function the same as the hashing function used to form the private-key-encrypted message digest, and also using the unencrypted event data in the header; and

means for comparing the trial message digest to the decrypted message digest to determine the authenticity of the image file,

wherein the event data includes location data.

40. An apparatus according to claim 39, wherein the location data comprises GPS-derived data.

41. An apparatus according to claim 39, wherein the means for obtaining the public key comprises means for obtaining the public key from a trusted party.

42. An apparatus according to claim 39, wherein the means for obtaining the public key comprises means for obtaining the public key from the header.

43. An apparatus according to claim 39, wherein said header includes camera information, and wherein said means for calculating a trial message digest comprises means for calculating the trial message digest using the camera information.

44. An apparatus according to claim 43, further comprising means for obtaining an identity of the hashing function from the header.

45. An apparatus for validating authenticity of an image file containing image data and a header that includes a private-key-encrypted message digest together with unencrypted data including event data that went into forming the message digest, comprising:

a program memory for storing process steps executable to: (1) obtain a public key complementary to a private key used to encrypt the message digest, (2) decrypt the private-key-encrypted message digest using the public key so as to obtain a message digest, (3) calculate a trial message digest using a hashing function the same as the hashing function used to form the private-key-encrypted message digest, and also using the unencrypted event data in the header, and (4) compare the trial message digest to the decrypted message digest to determine the authenticity of the image file, wherein the event data includes location data; and

a processor for executing the process steps stored in said memory.

46. An apparatus according to claim 45, wherein the location data comprises GPS-derived data.

47. An apparatus according to claim 45, wherein said step of obtaining the public key comprises the step of obtaining the public key from a trusted party.

48. An apparatus according to claim 45, wherein said step of obtaining the public key comprises the step of obtaining the public key from the header.

49. An apparatus according to claim 45, wherein said header includes camera information, and wherein said step of calculating a trial message digest comprises a step of calculating the trial message digest using the camera information.

50. A method according to claim 49, further comprising the step of obtaining an identity of the hashing function from the header.

51. Computer-executable process steps stored on a computer readable medium, said computer-executable process steps for validating authenticity of an image file containing image data and a header that includes a private-key-encrypted message digest together with unencrypted data including event data that went into forming the message digest, said computer-executable process steps comprising:

an obtaining step to obtain a public key complementary to a private key used to encrypt the message digest;

a decrypting step to decrypt the private-key-encrypted message digest using the public key so as to obtain a message digest;

a calculating step to calculate a trial message digest using a hashing function the same as the hashing function used to form the private-key-encrypted message digest, and also using the unencrypted event data in the header; and

a comparing step to compare the trial message digest to the decrypted message digest to determine the authenticity of the image file,

wherein the event data includes location data.

52. Computer-executable process steps according to claim 51, wherein the location data comprises GPS-derived data.

53. Computer-executable process steps according to claim 51, wherein said step of obtaining the public key comprises the step of obtaining the public key from a trusted party.

54. Computer-executable process steps according to claim 51, wherein said step of obtaining the public key comprises the step of obtaining the public key from the header.

55. Computer-executable process steps according to claim 51, wherein said header includes camera information, and wherein said step of calculating a trial message digest comprises a step of calculating the trial message digest using the camera information.

56. Computer-executable process steps according to claim 55, further comprising the step of obtaining an identity of the hashing function from the header.

57. A secure connection between a GPS receiver and a digital camera, whereby the digital camera can obtain secure GPS-derived data in correspondence to digital images obtained by the digital camera, comprising:

a private key encrypter in the GPS receiver, said private key encrypter for private-key-encryption of information corresponding to GPS-derived data;

a public key decrypter in the digital camera, said public key decrypter for public-key-decryption of the private-key-encrypted GPS-derived data; and

an interface between the GPS receiver and the digital camera for transmitting the private-key-encrypted GPS-derived data from the GPS receiver to the digital camera.

58. A secure connection between a GPS receiver and a digital camera according to claim 57, wherein said private key encrypter private-key-encrypts a message digest corresponding to the GPS-derived data.

59. A secure connection between a GPS receiver and a digital camera, according to claim 58, wherein the private key is secure with the GPS receiver, and wherein the public key is obtained from a trusted source and is complementary to the private key.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,269,446 B1
DATED : July 31, 2001
INVENTOR(S) : Thomas Schumacher et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 1,
Line 53, "Friedmin's" should read -- Friedman's --.

Column 3,
Line 5, "in" should read -- is --.

Column 4,
Line 27, "lo" should read -- **10** --.
Line 38, "result In" should read -- result. In --.

Column 5,
Line 6, "als" should read -- also --.
Line 20, "so" should read -- **50** --.

Signed and Sealed this

Twenty-sixth Day of March, 2002

Attest:

Attesting Officer

JAMES E. ROGAN
Director of the United States Patent and Trademark Office

US005504518A

United States Patent [19]

Ellis et al.

[11] Patent Number: 5,504,518

[45] Date of Patent: Apr. 2, 1996

[54] **METHOD AND SYSTEM FOR RECOGNITION OF BROADCAST SEGMENTS**

[75] Inventors: **Michael D. Ellis**; **Stephen M. Dunn**; **Michael W. Fellinger**; **Fancy B. Yonnglove**, all of Boulder; **David M. James**, Fort Collins; **David L. Clifton**, Boulder; **Richard S. Land**, Lafayette, all of Colo.

[73] Assignee: **The Arbitron Company**, Columbia, Md.

[21] Appl. No.: **474,248**

[22] Filed: **Jun. 7, 1995**

Related U.S. Application Data

[62] Division of Ser. No. 876,578, Apr. 30, 1992, Pat. No. 5,436,653.

[51] **Int. Cl.**[6] **H04N 17/00**; H04N 17/04

[52] **U.S. Cl.** **348/2**; 348/907; 455/2

[58] **Field of Search** 348/2, 3, 907; 455/2, 67; H04N 17/00, 17/04, 17/06

[56] **References Cited**

U.S. PATENT DOCUMENTS

2,766,374	10/1956	Hoffman .
3,919,479	11/1975	Moon .
4,025,851	5/1977	Haselwood et al. .
4,230,990	10/1980	Lert, Jr. et al. .
4,450,531	5/1984	Kenyon et al. .
4,547,804	10/1985	Greenberg .
4,599,644	7/1986	Fischer .
4,639,799	1/1987	Inoue .
4,677,466	6/1987	Lert, Jr. et al. .
4,697,209	9/1987	Kiewit et al. .
4,718,106	1/1988	Weinblatt .
4,739,398	4/1988	Thomas et al. .
4,750,034	6/1988	Lem .
4,843,562	6/1989	Kenyon et al. .
4,857,999	8/1989	Welsh .
4,918,730	4/1990	Schulze .
4,931,871	6/1990	Kramer .
4,945,412	7/1990	Kramer .
4,955,070	9/1990	Welsh et al. .
4,967,273	10/1990	Greenberg .
5,019,899	5/1991	Boles et al. .
5,023,929	6/1991	Call .

OTHER PUBLICATIONS

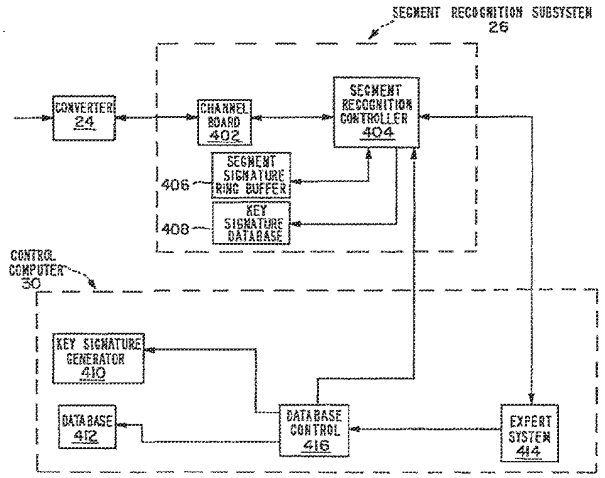
Gonzalez & Wintz, *Digital Image Processing*, 1987, title page, copyright page and pp. 122–130.

Primary Examiner—James J. Groody
Assistant Examiner—Glenton B. Burgess
Attorney, Agent, or Firm—Curtis, Morris & Safford; Eugene L. Flanagan, III

[57] **ABSTRACT**

The broadcast audio signal and/or the broadcast video signal of a monitored broadcast are temporarily stored and predetermined signal events are detected which indicate possible new broadcast segments of interest of the monitored broadcast. Intervals of the monitored broadcast are selected as possible new broadcast segments of interest based on the predetermined signal events. A first capture level is assigned to a first selected interval based on predetermined characteristics of the interval which indicate that it is likely to be a new segment of interest. A second capture level is assigned to a second selected interval based on predetermined characteristics of that interval which indicate that it is relatively less likely than the first selected interval to be a new segment of interest. A signature corresponding with the first selected interval is stored in the database and the temporarily stored broadcast audio and/or video signals which correspond with the first selected interval are captured for transmission to a workstation operator for segment identification. A signature corresponding with the second selected interval is stored in the database and the temporarily stored broadcast audio and/or video signals which correspond with the second selected interval are erased.

3 Claims, 19 Drawing Sheets



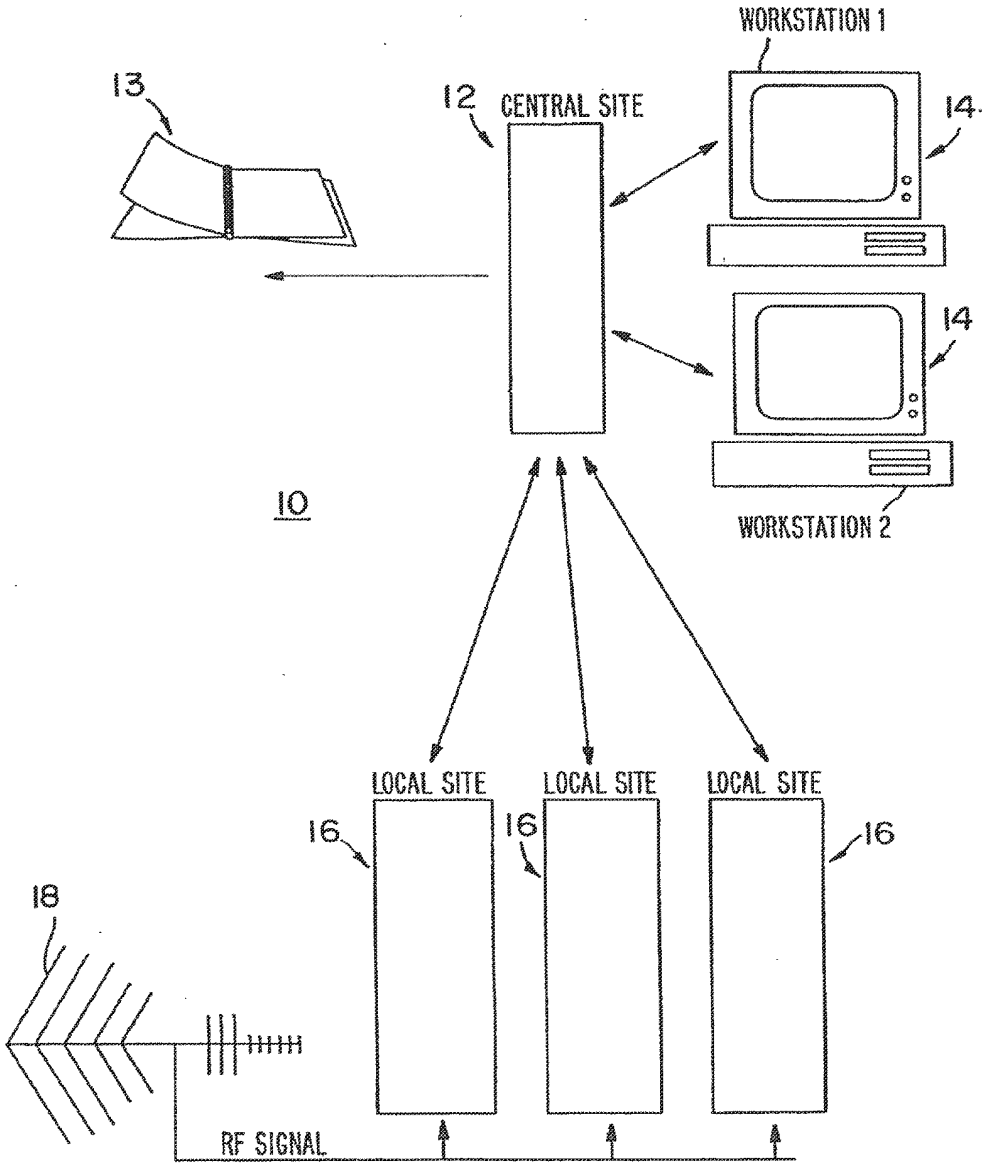

WORKSTATION 1
13
12
CENTRAL SITE
14
14
10
WORKSTATION 2
LOCAL SITE
LOCAL SITE
LOCAL SITE
16
16
16
18
RF SIGNAL

FIG. 1

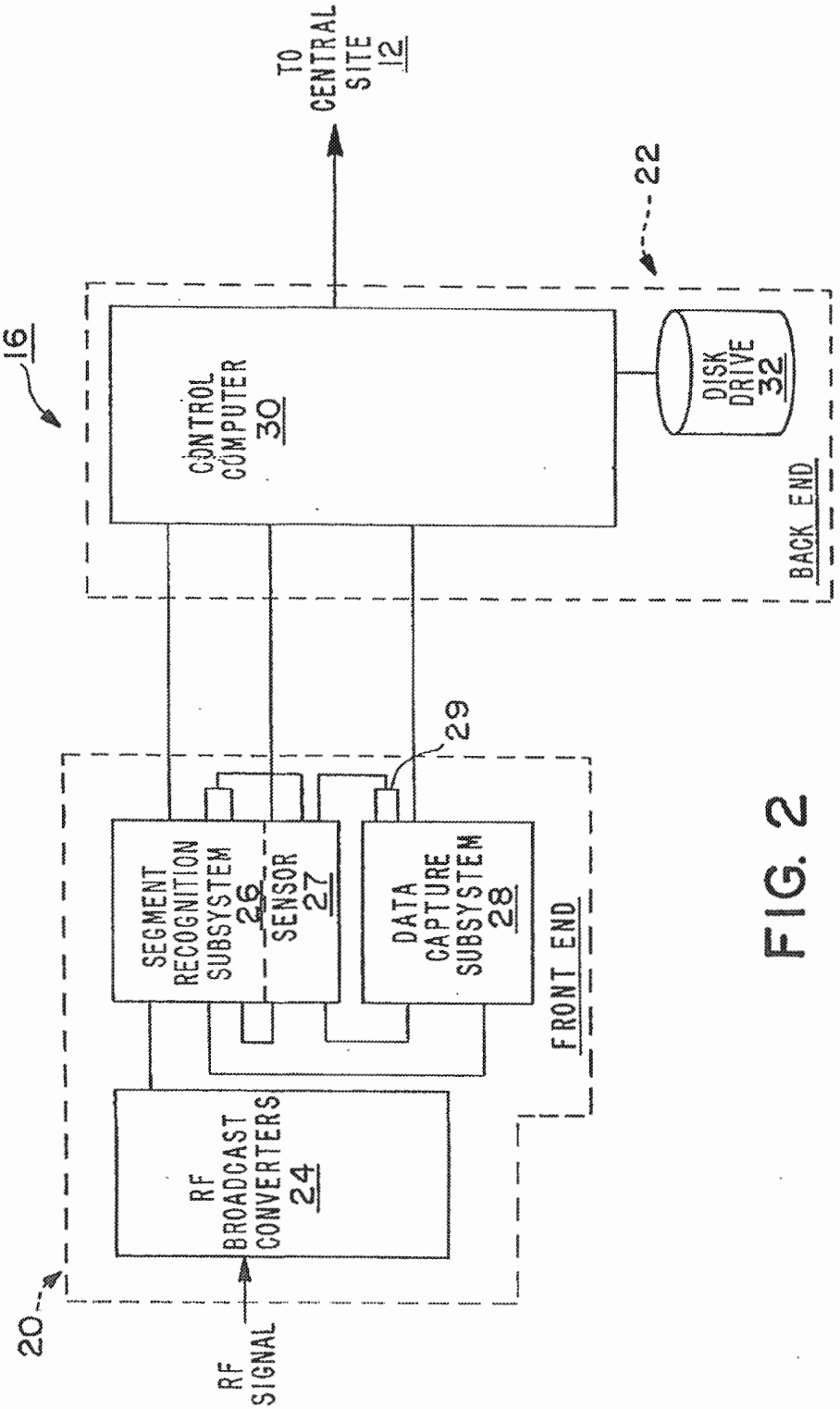
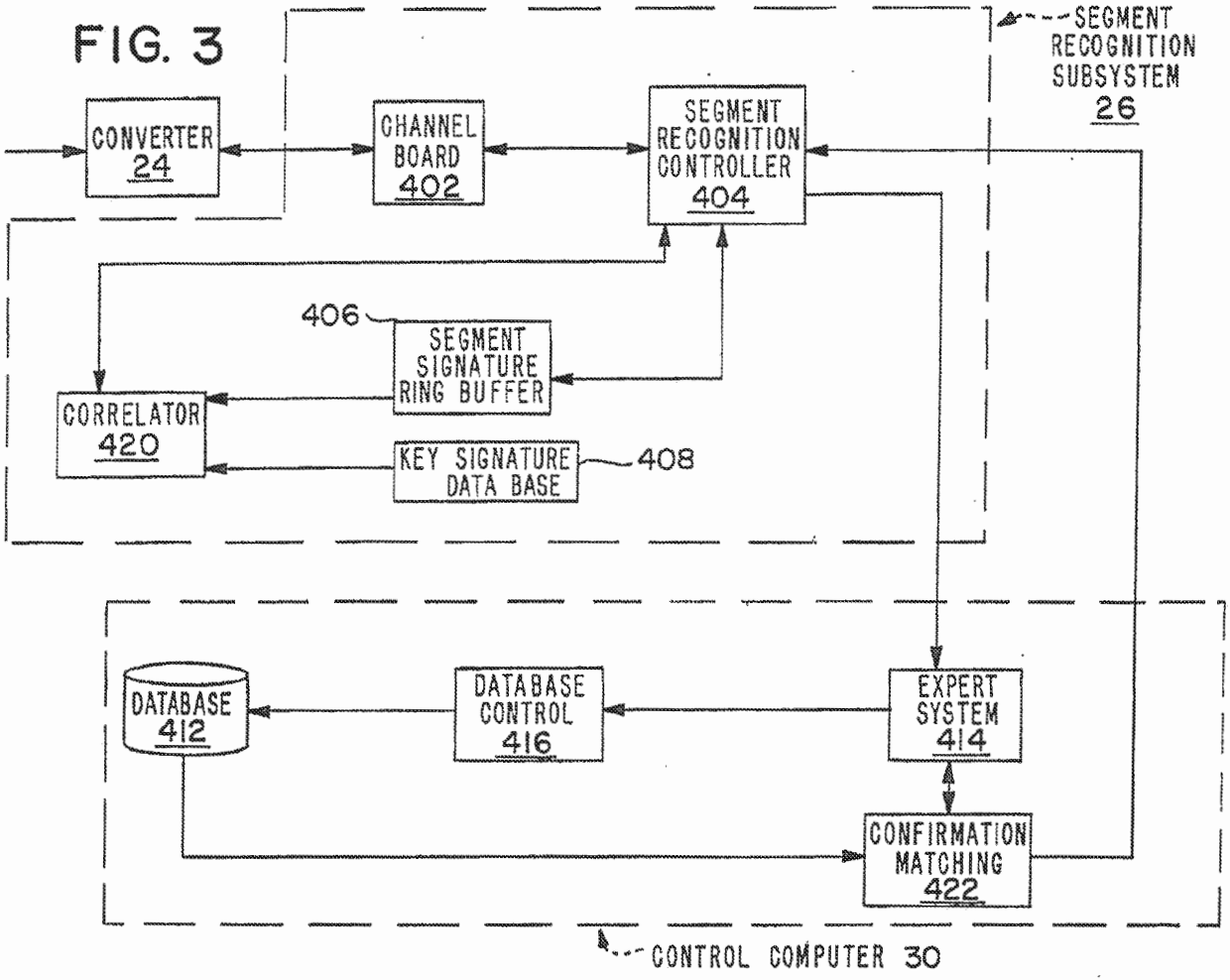


FIG. 2

ADOBE – Exhibit 1002, page 169

FIG. 3



JAFFE-ADOBE00204

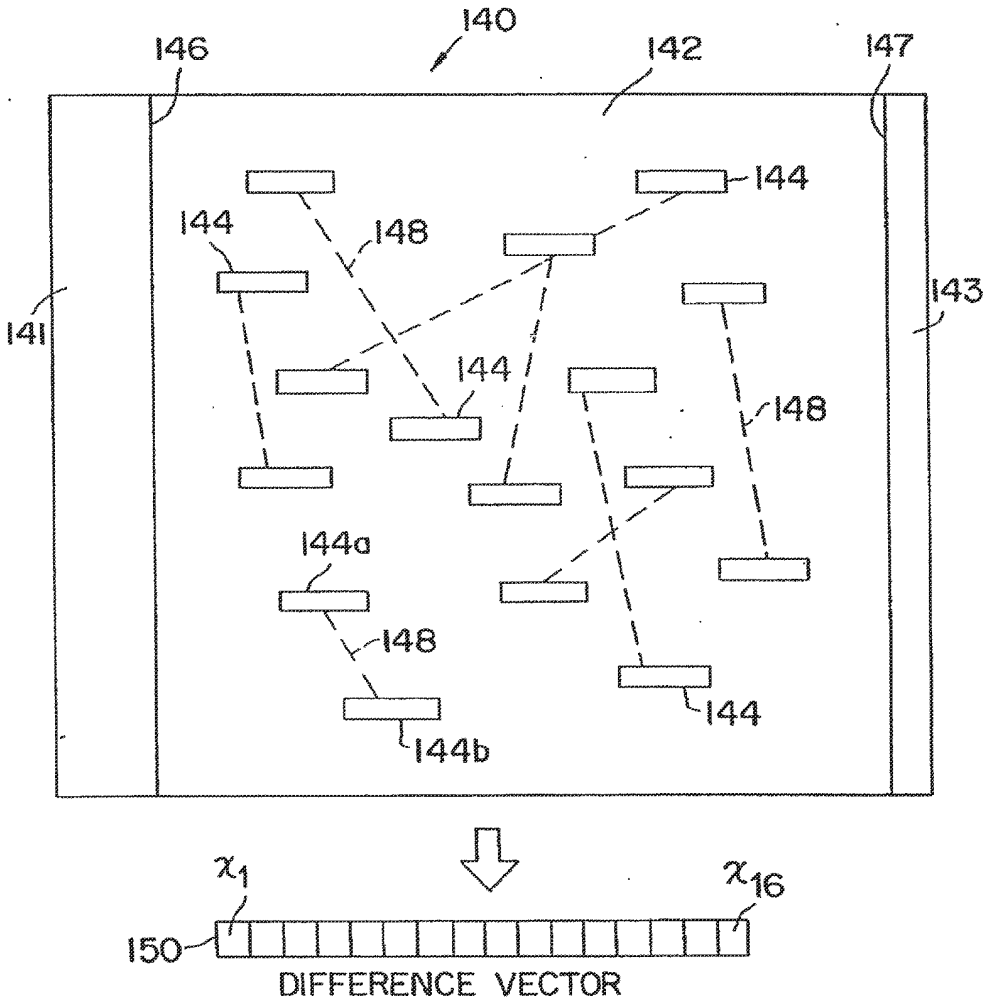

140
146
142
147
144
144
148
141
143
144
148
144a
148
144
144b
x_1
x_{16}
150
DIFFERENCE VECTOR

FIG. 4

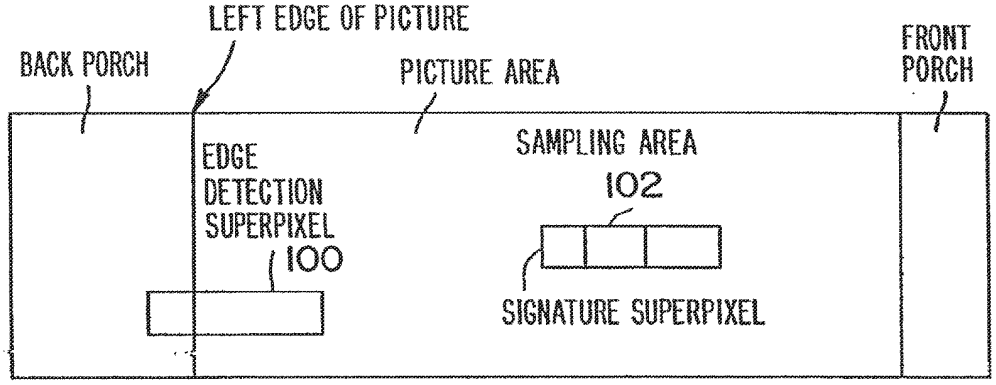

LEFT EDGE OF PICTURE
BACK PORCH
PICTURE AREA
FRONT PORCH
EDGE DETECTION SUPERPIXEL
100
SAMPLING AREA
102
SIGNATURE SUPERPIXEL

FIG. 5A

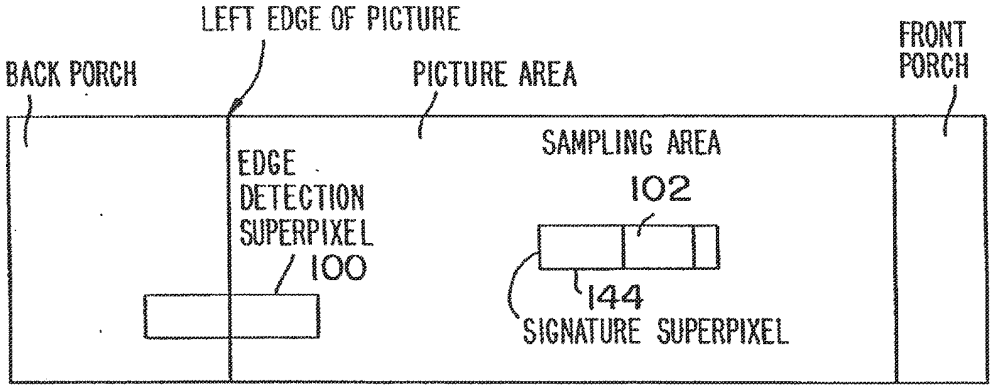

LEFT EDGE OF PICTURE
BACK PORCH
PICTURE AREA
FRONT PORCH
EDGE DETECTION SUPERPIXEL
100
SAMPLING AREA
102
144
SIGNATURE SUPERPIXEL

FIG. 5B

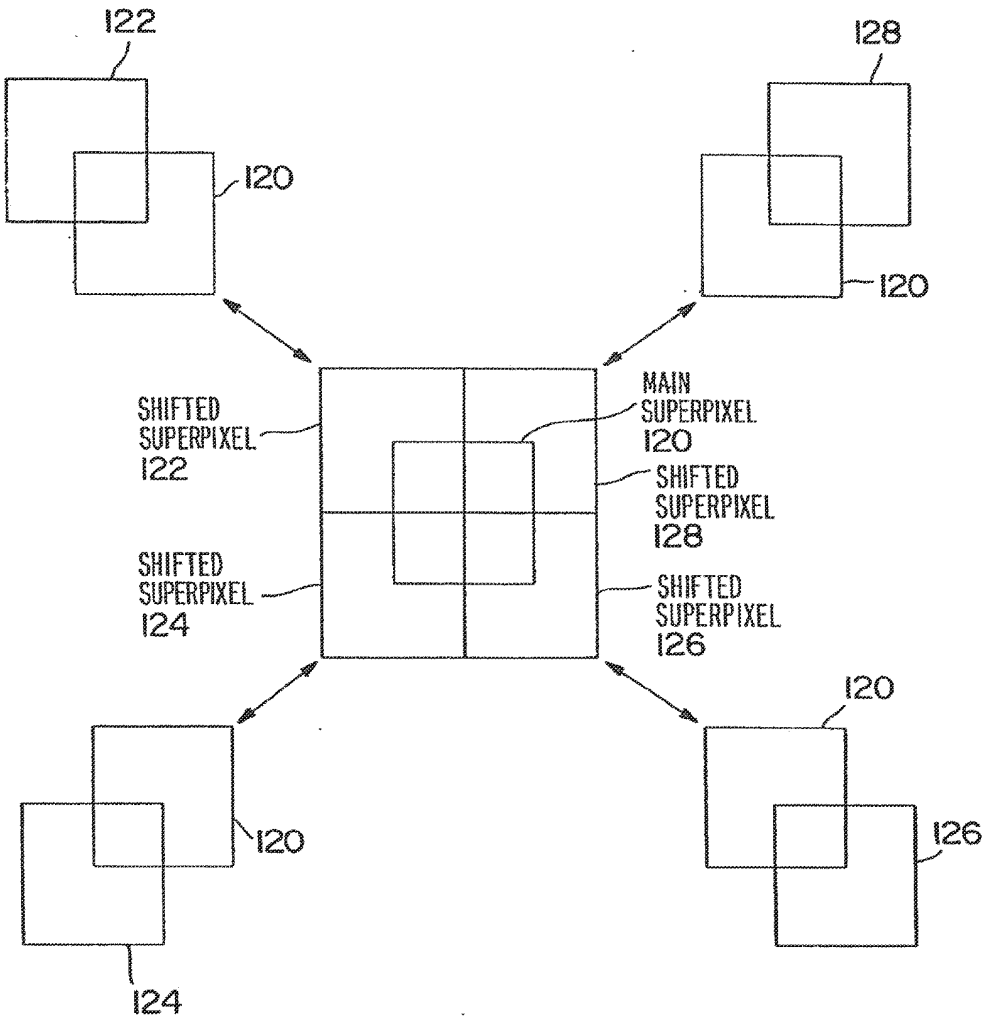

122
128
120
120
SHIFTED SUPERPIXEL 122
MAIN SUPERPIXEL 120
SHIFTED SUPERPIXEL 128
SHIFTED SUPERPIXEL 124
SHIFTED SUPERPIXEL 126
120
120
126
124

FIG.6

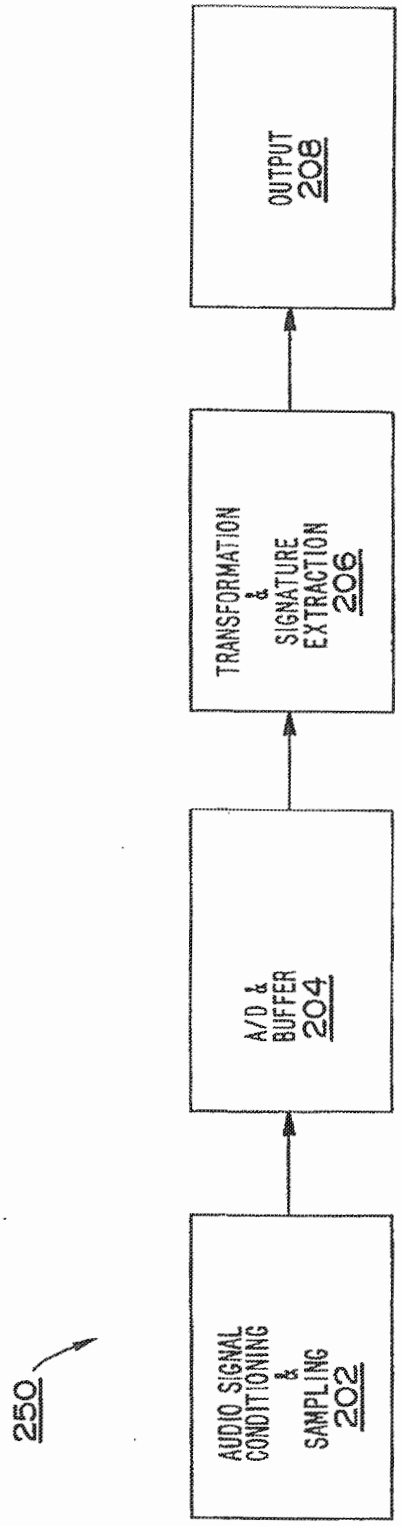


FIG. 7A

ADOBE – Exhibit 1002, page 174

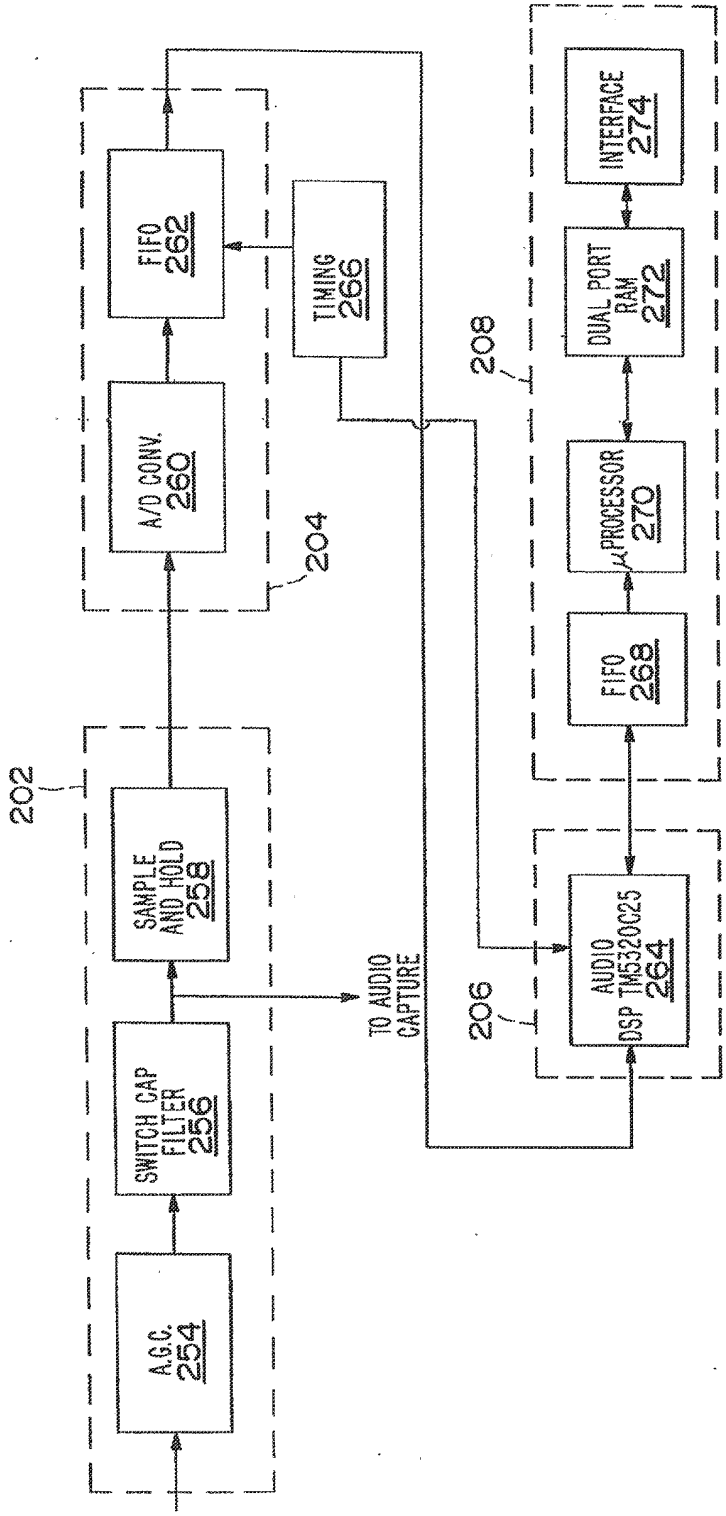


FIG. 7B

ADOBE – Exhibit 1002, page 175

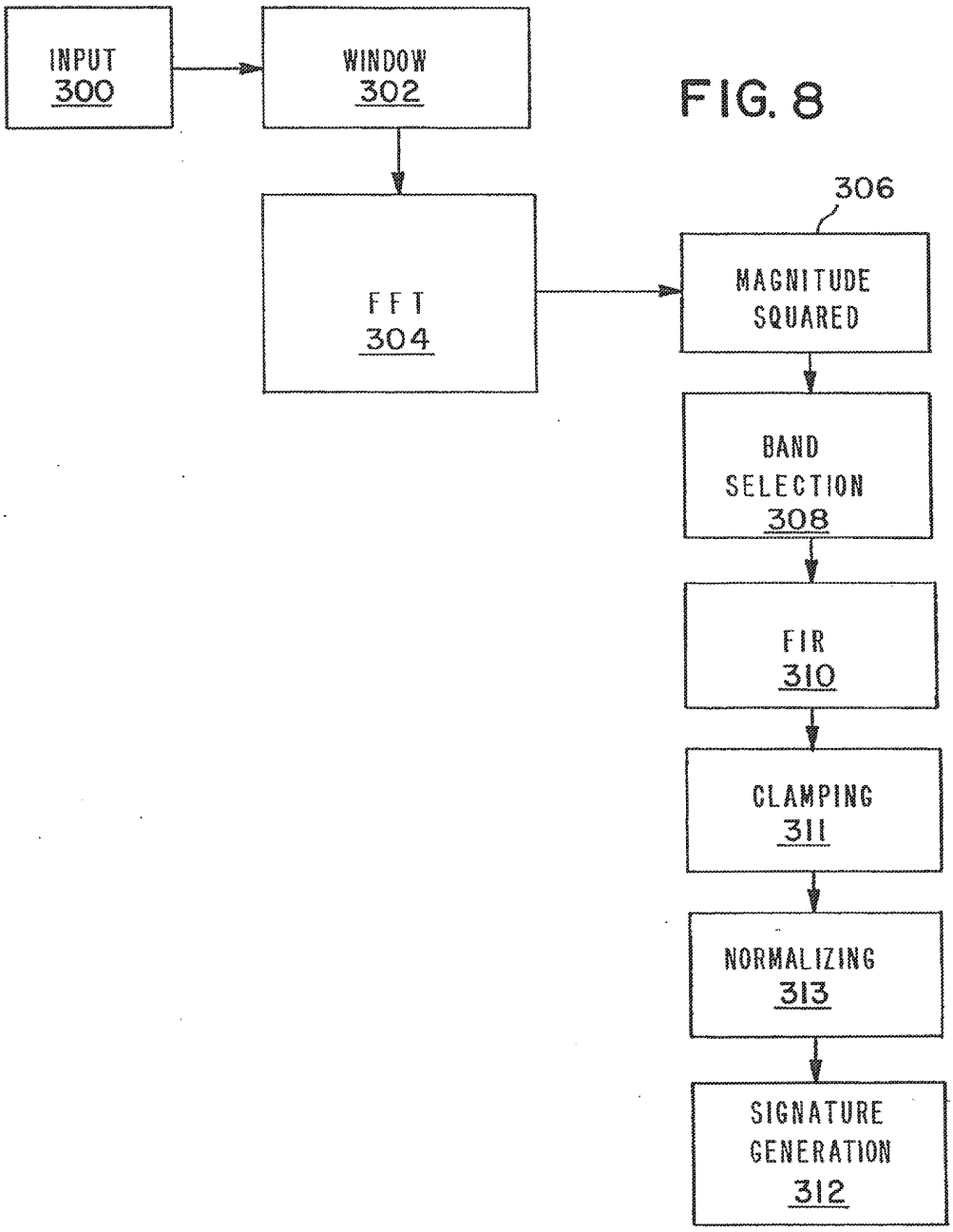

INPUT
300
WINDOW
302
FFT
304
306
MAGNITUDE
SQUARED
BAND
SELECTION
308
FIR
310
CLAMPING
311
NORMALIZING
313
SIGNATURE
GENERATION
312

FIG. 8

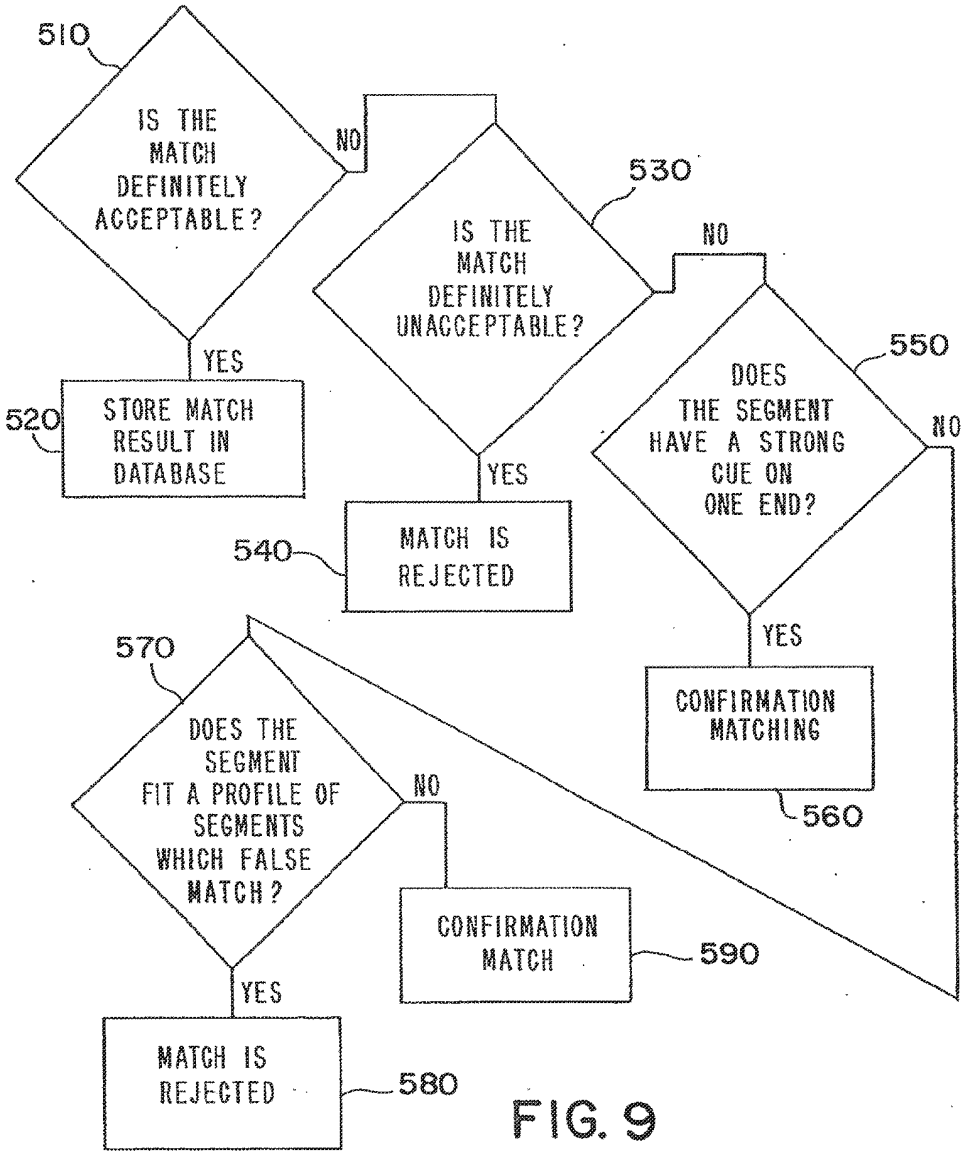

510
IS THE MATCH DEFINITELY ACCEPTABLE?
NO
YES
520
STORE MATCH RESULT IN DATABASE
530
IS THE MATCH DEFINITELY UNACCEPTABLE?
NO
YES
540
MATCH IS REJECTED
550
DOES THE SEGMENT HAVE A STRONG CUE ON ONE END?
NO
YES
CONFIRMATION MATCHING
560
570
DOES THE SEGMENT FIT A PROFILE OF SEGMENTS WHICH FALSE MATCH?
NO
YES
CONFIRMATION MATCH
590
MATCH IS REJECTED
580

FIG. 9

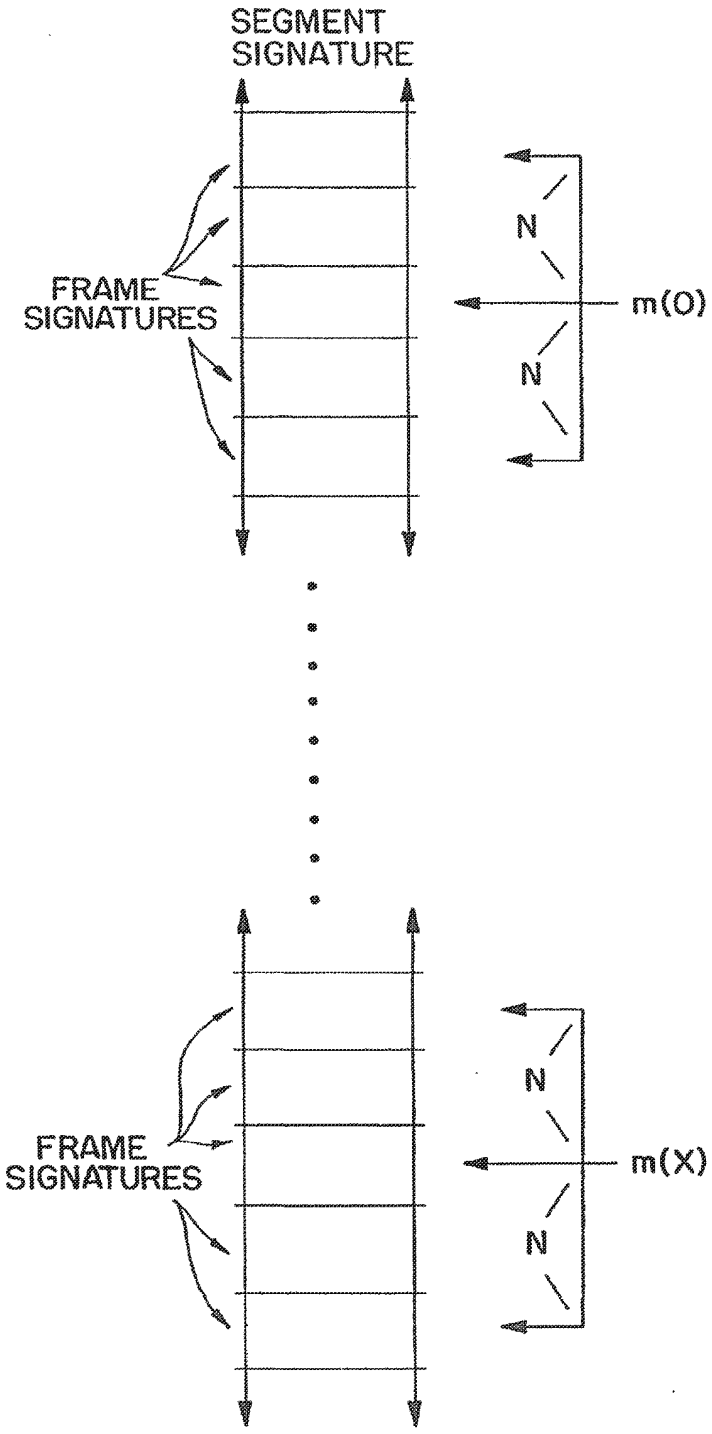

SEGMENT SIGNATURE
FRAME SIGNATURES
N
m(O)
N
FRAME SIGNATURES
N
m(X)
N

FIG. 10

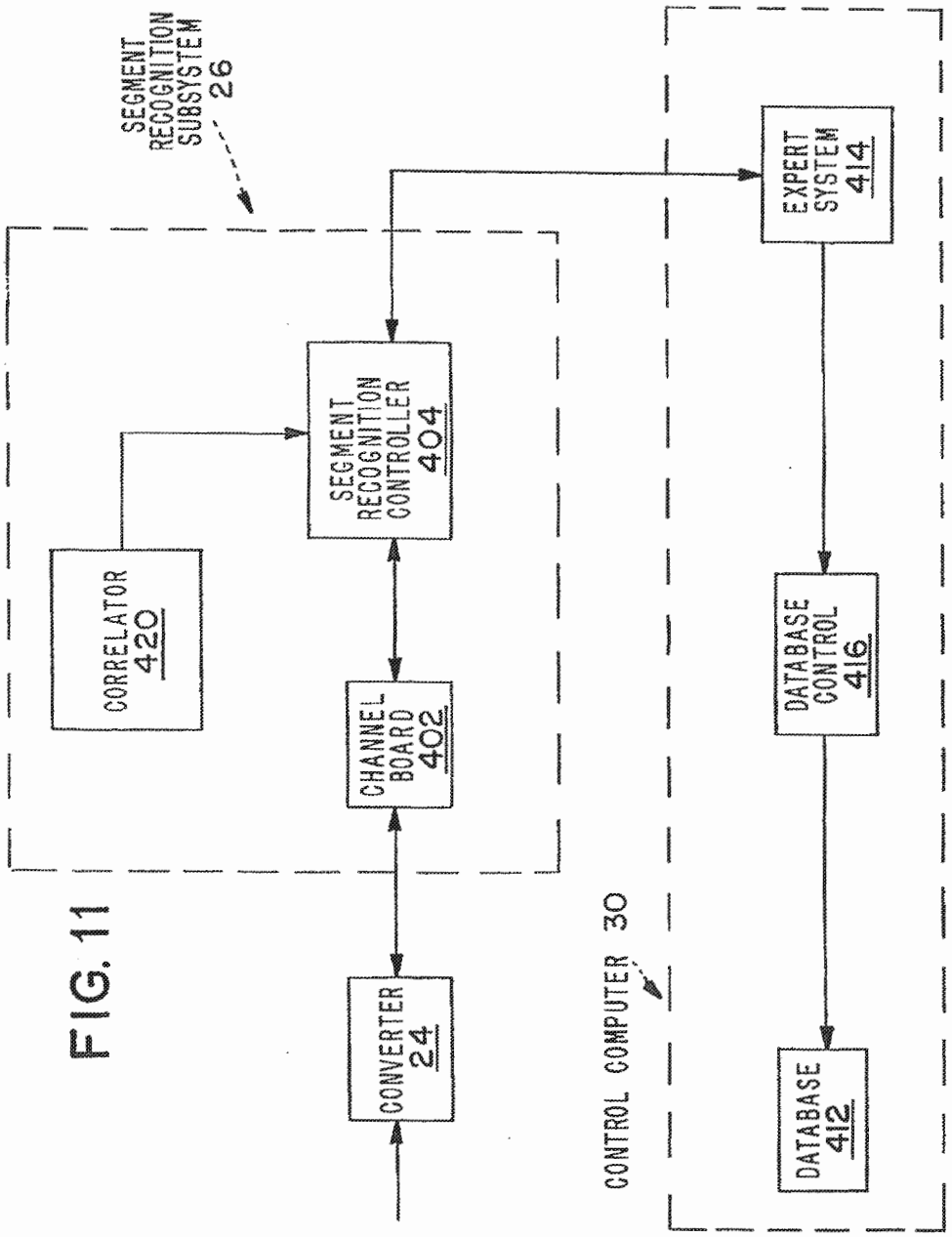


FIG. 11

ADOBE – Exhibit 1002, page 179

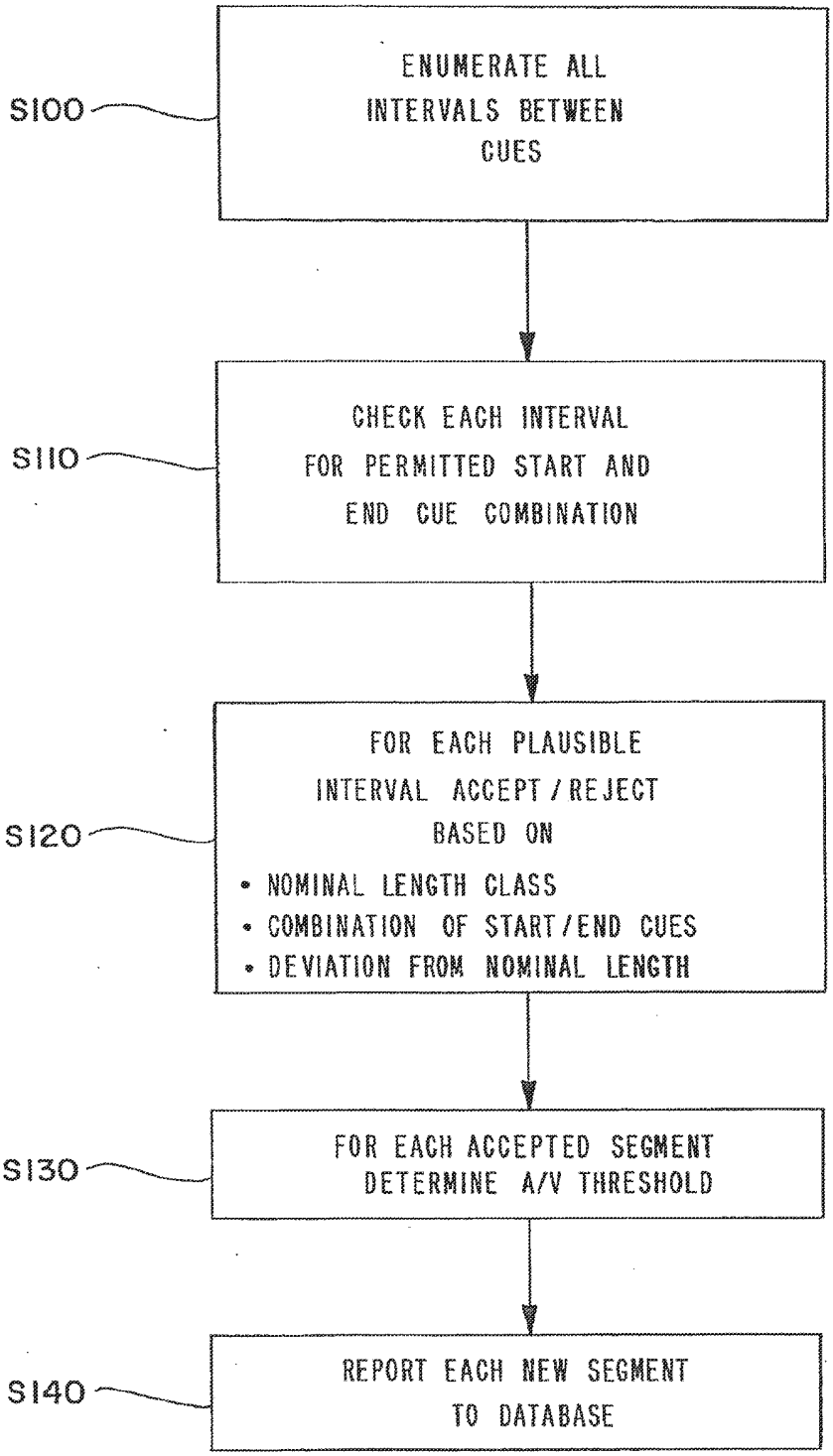

S100
ENUMERATE ALL INTERVALS BETWEEN CUES
S110
CHECK EACH INTERVAL FOR PERMITTED START AND END CUE COMBINATION
S120
FOR EACH PLAUSIBLE INTERVAL ACCEPT / REJECT BASED ON
• NOMINAL LENGTH CLASS
• COMBINATION OF START / END CUES
• DEVIATION FROM NOMINAL LENGTH
S130
FOR EACH ACCEPTED SEGMENT DETERMINE A/V THRESHOLD
S140
REPORT EACH NEW SEGMENT TO DATABASE

FIG. 12

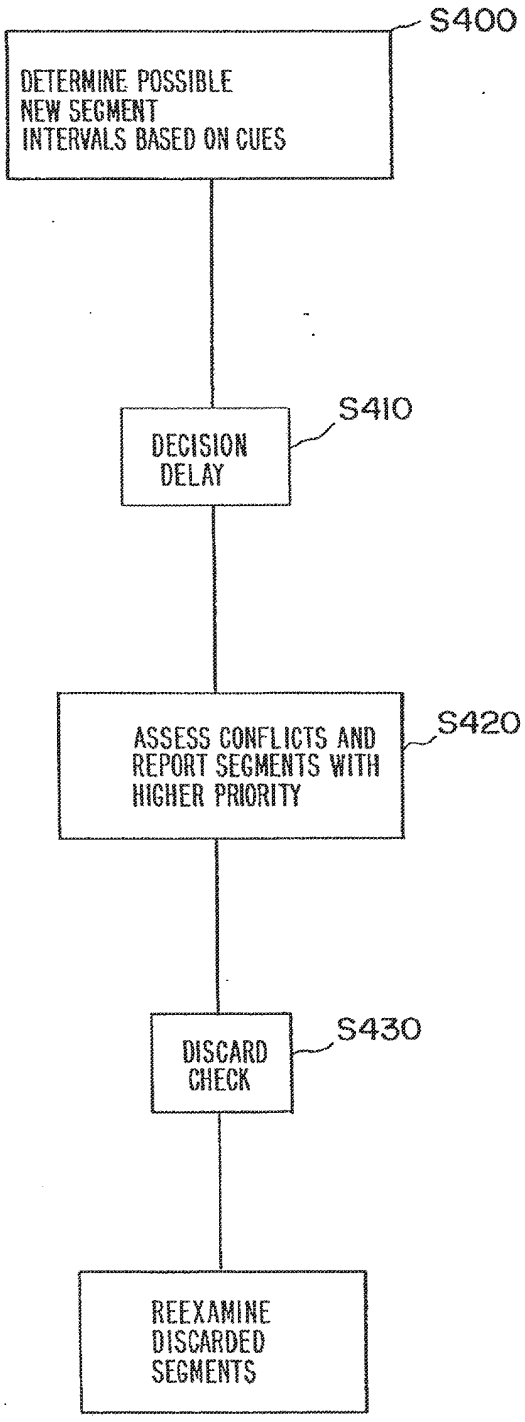

S400
DETERMINE POSSIBLE NEW SEGMENT INTERVALS BASED ON CUES
S410
DECISION DELAY
S420
ASSESS CONFLICTS AND REPORT SEGMENTS WITH HIGHER PRIORITY
S430
DISCARD CHECK
REEXAMINE DISCARDED SEGMENTS

FIG.13

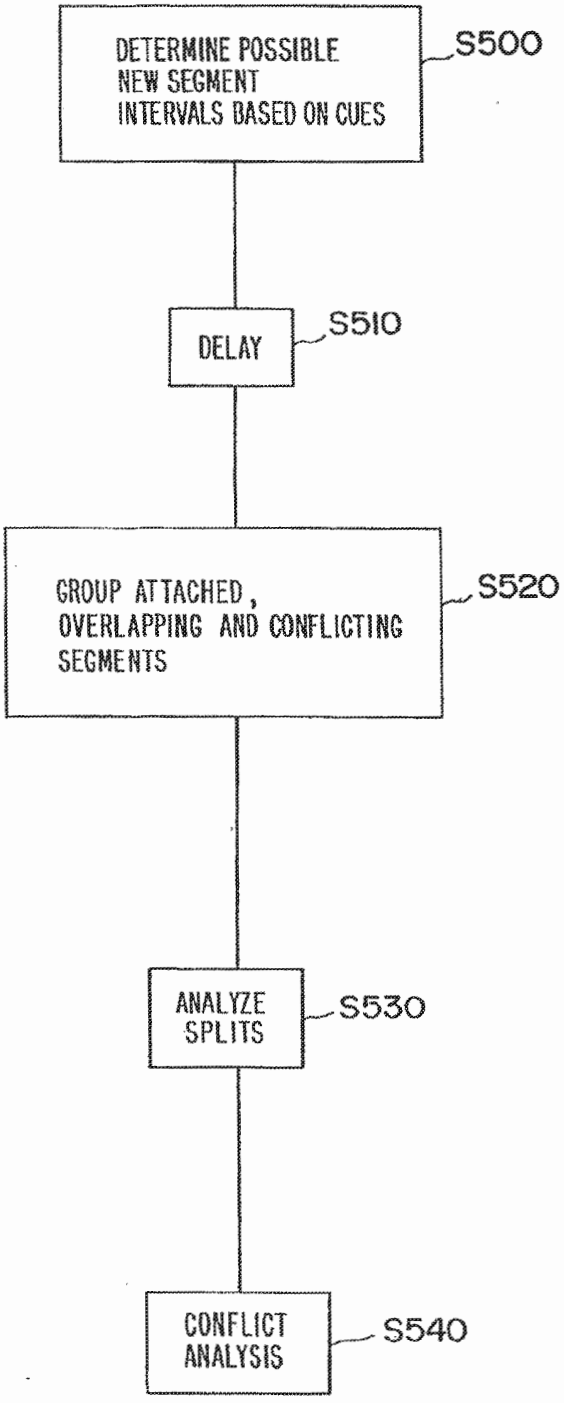

DETERMINE POSSIBLE NEW SEGMENT INTERVALS BASED ON CUES
S500
DELAY
S510
GROUP ATTACHED, OVERLAPPING AND CONFLICTING SEGMENTS
S520
ANALYZE SPLITS
S530
CONFLICT ANALYSIS
S540

FIG. 14

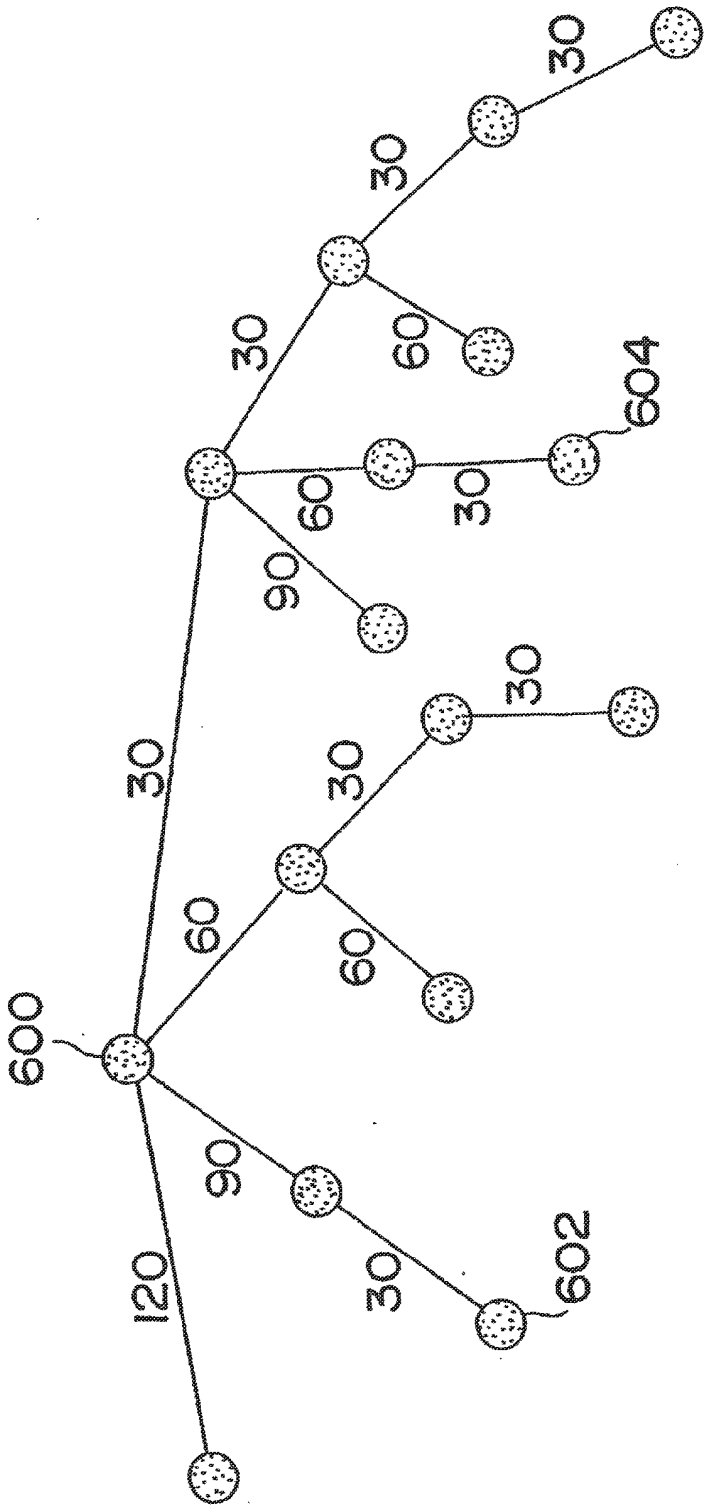
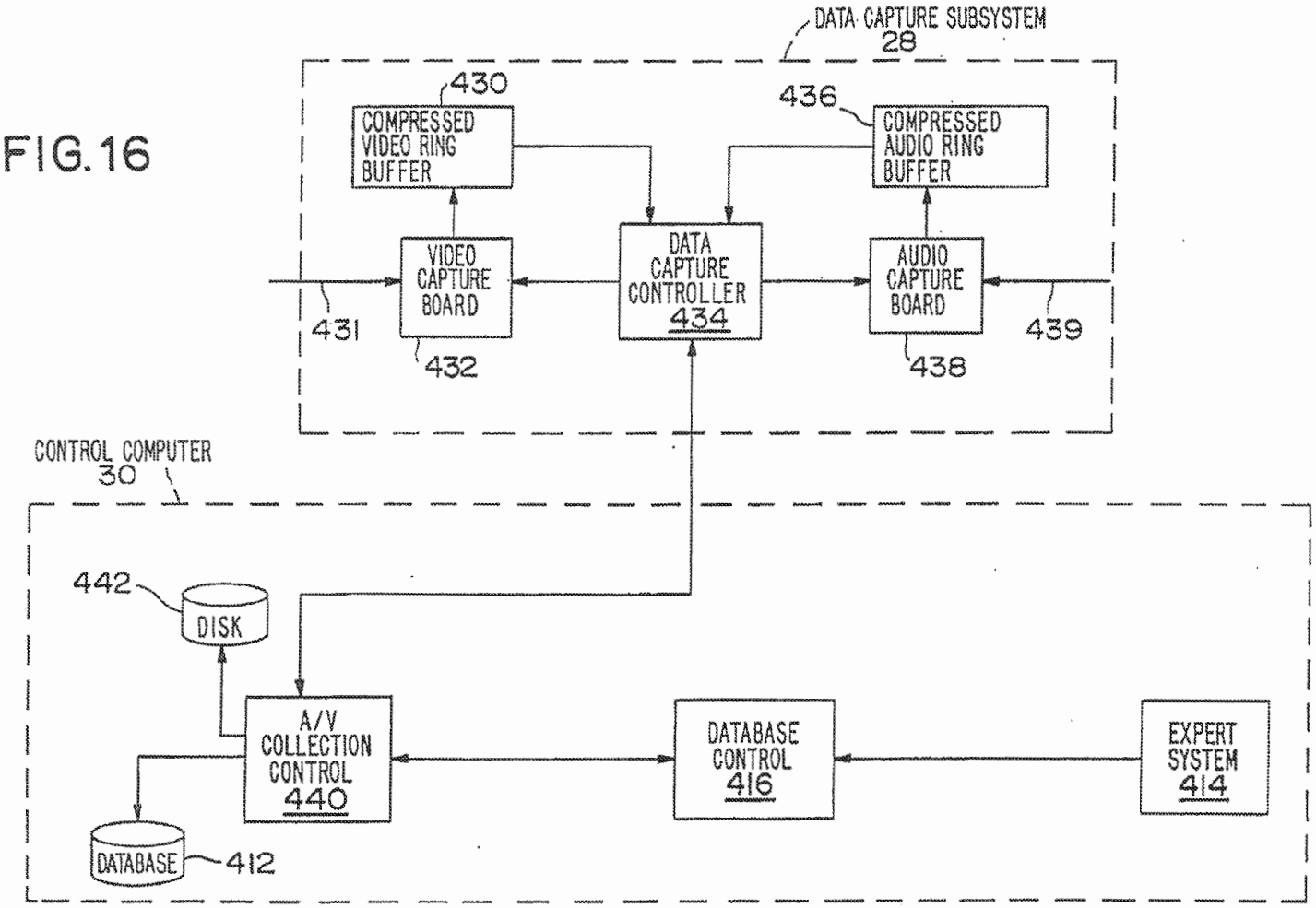


FIG. 15

FIG. 16



JAFFE-ADOBE00218

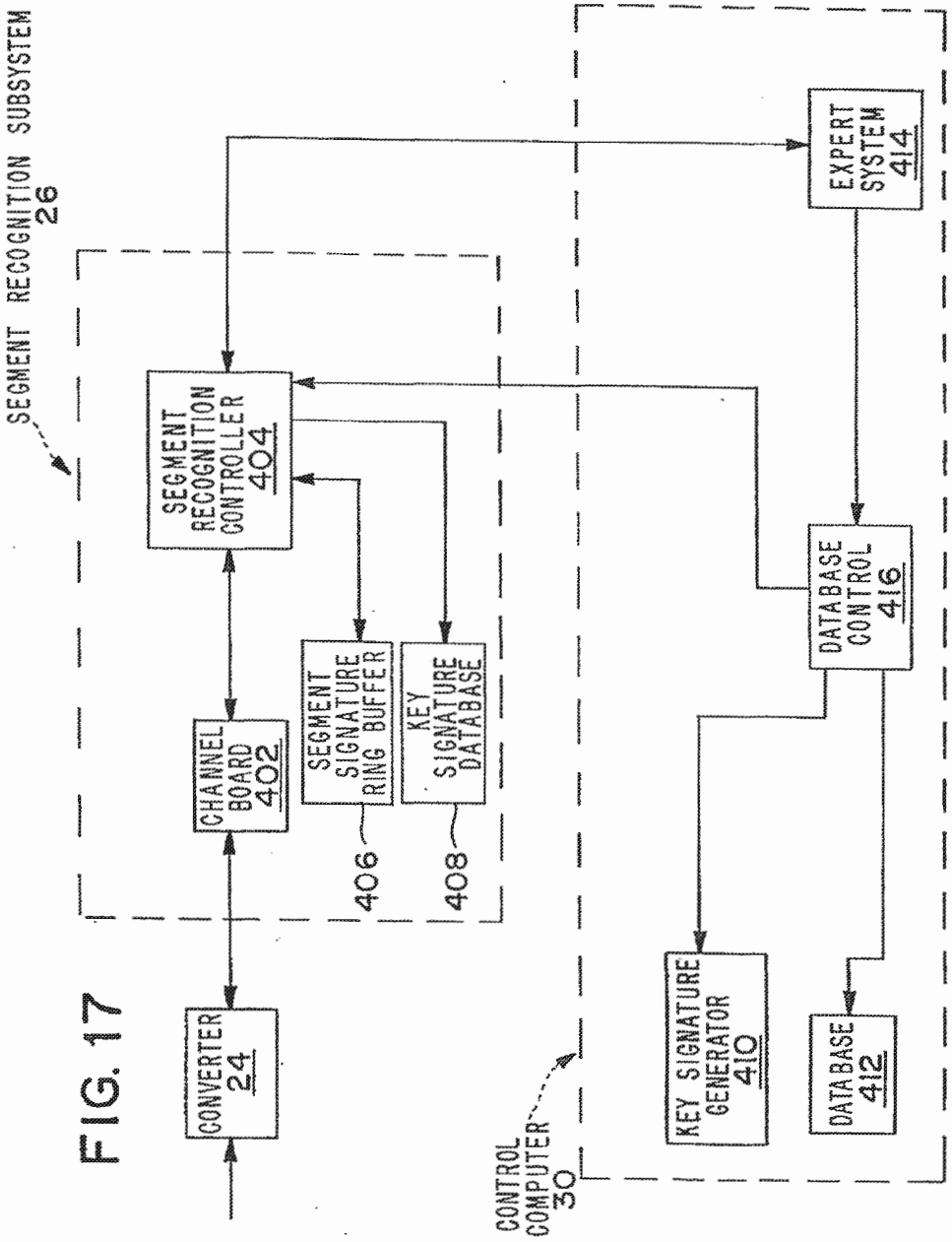


FIG. 17

ADOBE – Exhibit 1002, page 185

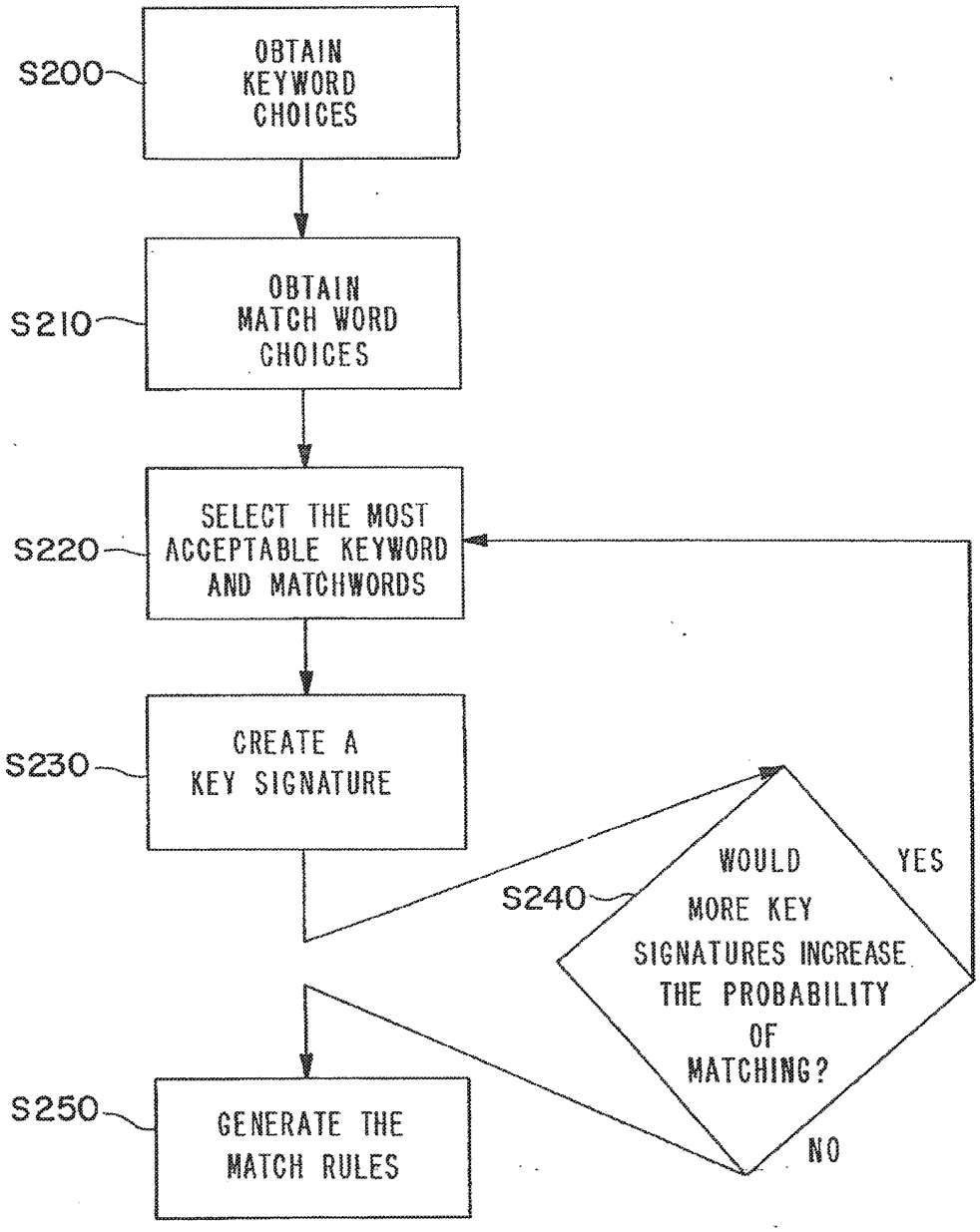

S200
OBTAIN KEYWORD CHOICES
S210
OBTAIN MATCH WORD CHOICES
S220
SELECT THE MOST ACCEPTABLE KEYWORD AND MATCHWORDS
S230
CREATE A KEY SIGNATURE
S240
WOULD MORE KEY SIGNATURES INCREASE THE PROBABILITY OF MATCHING?
YES
NO
S250
GENERATE THE MATCH RULES

FIG. 18

METHOD AND SYSTEM FOR RECOGNITION OF BROADCAST SEGMENTS

This application is a division of application Ser. No. 07/876,578, filed Apr. 30, 1992, now U.S. Pat. No. 5,436,653.

BACKGROUND OF THE INVENTION

The present invention relates to the automatic recognition of widely disseminated signals, such as television and radio broadcasts, and the like.

Broadcast advertisers need to confirm that their advertisements have been aired in their entireties by designated broadcast stations and at the scheduled times. Further, it may be desirable for advertisers to know what advertisements their competitors have aired. A conventional technique for monitoring the advertisements that have been aired involves employing a large number of people to watch designated broadcast channels over the course of the day in order to record this information in a written diary. It will be appreciated that this conventional technique involves the need to employ a large number of people as well as the need to gather their written records and to enter their contents in an automatic data processing system in order to produce reports of interest to particular advertisers. Such conventional technique has a relatively high recurring cost. In an attempt to reduce such costs, an automatic pattern recognition system has been developed as, for example, that disclosed in U.S. Pat. No. 4,739,398.

In the continuous pattern recognition technique disclosed in U.S. Pat. No. 4,739,398, a segment or portion of a signal may be identified by continuous pattern recognition on a real-time basis. The signal may be transmitted, for example, over-the-air, via satellite, cable, optical fiber, or any other means effecting wide-dissemination thereof.

For example, in the case of a television broadcast signal the video signal is parametized so as to produce a digital data stream having one 16-bit digital word for each video frame which, in the NTSC system, occurs every 1/30 of a second. It will be appreciated that different signal intervals, such as video fields, may instead be parametized in this fashion. These digital words are compared to digital words representing commercials or other segments of interest which are stored in a storage device. Information relating to each match that is detected therebetween (which indicates that a segment of interest has been broadcast) is collected.

More specifically, a digital key signature is generated for each known segment (e.g., commercial) which is to be recognized or matched. The key signature advantageously includes eight 16-bit words or match words which are derived from eight frames of broadcast information which are selected from among the frames contained within the desired segment in accordance with a predetermined set of rules, together with offset information indicating the spacing (measured, for example, in frames or fields) between the location of the frame represented by each word of the signature and that represented by the first word thereof. In the case of a video signal, thirty-two predetermined areas thereof comprising, for example, eight by two pixels from each frame (or one selected field thereof representing each frame) are selected, for example. An average luminance value for the pixels of each area is produced and compared with the average luminance value of an area paired therewith. The result of such comparison is normalized to a bit value of one or zero based on a determination whether the average luminance value of a first one of the areas is either (i) greater than or equal to, or (ii) less than, the average luminance value of the second one of the areas. In this fashion, a sixteen bit frame signature is produced for each frame of the video signal.

A sixteen bit mask word is also produced for each sixteen bit frame signature. Each bit of the mask word represents the susceptibility of a corresponding bit of the frame signature to noise, and is produced on the basis of the difference between the average luminance values of the respective areas used to produce the corresponding bit of the frame signature. That is, if the absolute value of the difference between such average luminances values is less than a guard band value, the corresponding mask bit is set, indicating susceptibility to noise.

The eight match words are selected from the above-described frame signatures of each segment and stored, together with their mask words and offset information, as part of the key signature for that segment.

The received signal to be recognized is digitized and a 16-bit frame signature is produced in the manner described above for each frame (or selected field) of data. After the incoming signals are received and processed, they are read into a buffer which holds a predetermined amount of data. Each 16-bit frame signature from the incoming signal is assumed to correspond with the first word of one of the previously stored eight-word key signatures. As such, each received word is compared to all key signatures beginning with that word. Using the offset information stored with the signatures, subsequent received frame signatures (which are already in the buffer) are compared to the corresponding match words in the key signature to determine whether or not a match exists.

More specifically, each match word of the key signature is paired with a respective frame signature of the received signature based on the offset information and corresponding bits of the paired match words and frame signatures are compared. A total error count is produced based on this comparison as follows. If corresponding bits of the match word and frame signature are unmasked, then an error count of zero is accumulated when these bits are the same in value and an error count of one is accumulated if these bits differ in value. If the bits are masked, then an error count of one-half is accumulated therefor regardless of the bit values. A total error count is accumulated for all match words and corresponding frame signatures and, if the total error count is less than a predetermined default or error threshold, a match is found. Otherwise, no match is found.

As will be appreciated, in order to perform the above exemplary processing in real time, all comparisons should be completed within the time associated with each data frame, that is, within 1/30 of a second. Typical processing speed, associated with normal processing devices, will allow only a limited number of segment signatures to be stored and used for comparison.

The speed with which a key signature can be compared to a segment signature for a newly received broadcast may be substantially increased by utilizing a keyword look-up data reduction method. In this method, one frame is selected from the frames contained within the segment corresponding to the key signature, in accordance with a set of predetermined criteria. Such selected frame is a key frame and the frame signature associated therewith is the keyword. The key signature still preferably has eight 16-bit words, however, the offset information relating thereto now represents spac-

ing from the keyword, rather than a spacing from the first word in the key signature.

The keyword may be one of the key signature words within the key signature, in which situation the offset for that word has a value of 0, or it may be a ninth word. The frame location of the keyword does not need to temporally precede the frame locations of all of the other match words within the key signature.

There may be multiple key signatures associated with each keyword. As an example, if 16-bit words are utilized and if four key signatures are associated with each keyword, then four complete signature comparisons would be the maximum number that would have to be performed within the 1/30 of a second time limit (assuming no data errors). Such number of comparisons is readily performed within the time limit.

It is desired to achieve the highest possible accuracy in broadcast segment recognition, as well as the greatest possible efficiency. However, a number of problems are encountered in carrying out such a technique. For example, broadcast signals are subject to time shifts such as a shift in the edge of a video picture which occurs from time to time. Video signals are also subject to jitter. Each of these effects will adversely impact a segment recognition technique relying upon sampling predetermined portions of the video signal, unless these effects are somehow compensated.

A further difficulty encountered in carrying out broadcast segment recognition based upon video signals is that the signatures which they generate tend to be distributed unevenly in value due to the similarities between video signals of different segments. Accordingly, video signatures tend to be distributed unevenly so that relatively large numbers of signatures tend to have similar values and are, thus, prone to false match (that is, indicate a match between signatures representing different segments).

Heretofore, it has been thought impractical to carry out pattern recognition of audio broadcast segments due to the difficulties encountered in extracting sufficient information from audio signals. For example, television audio signals are predominantly speech signals which are concentrated below approximately 3,000 Hz and possess very similar frequency spectra from one segment to the next.

Due to the foregoing effects, as well as signal noise, it is difficult to implement a pattern recognition technique for broadcast segment identification which possesses high accuracy. That is, the possibilities that segment signatures either will false match or fail to provide a completely reliable match tends to limit the accuracy of such a technique. Where, for example, known segments are not identified by the pattern recognition system, they may be transmitted to a workstation operator for identification as potential new segments, when in fact they are not. The result is that workstation operator time is wasted and system efficiency is degraded. On the other hand, if new segments are identified when in fact they are not segments of interest, workstation operator time may also be wasted in a useless attempt to identify such segments. For example, in a television commercial recognition system, it is necessary to distinguish television commercials from normal programming, news breaks, public service announcements, etc. It is, therefore, desirable to ensure that the greatest number of new segments provided to workstation operators for identification are in fact segments of interest. A further difficulty is encountered where new segments of interest are incorrectly split, so that portions of new segments only are reported to the workstation operators which may prevent correct identification of the segment which also wastes the operator's time.

OBJECTS AND SUMMARY OF THE INVENTION

It is an object of the present invention to provide methods and apparatus for use in broadcast segment recognition and the like providing improved recognition accuracy and system efficiency.

In accordance with an aspect of the present invention, a broadcast segment recognition system and method comprise means for and the steps of, respectively, producing a signature for each of a plurality of broadcast segments to be recognized; storing each said signature to form a database of broadcast segment signatures; monitoring a broadcast segment; forming a signature representing the monitored broadcast segment; comparing the signature representing the monitored broadcast segment with at least one of the broadcast segment signatures of the database to determine whether a match exists therebetween; and evaluating the validity of a match of a monitored broadcast segment by carrying out at least one of: (a) determining whether the monitored broadcast segment is temporally bounded by predetermined signal events; (b) determining whether the monitored broadcast segment overlaps another monitored broadcast segment for which a match has been accepted in accordance with predetermined criteria; and (c) determining whether the match conforms with a predetermined profile of false matching segments.

In accordance with another aspect of the present invention, a system and method for broadcast segment recognition are provided comprising means for and the steps of, respectively, producing a signature for each of a plurality of broadcast segments to be recognized; storing each said signature to form a database of broadcast segment signatures; monitoring a broadcast segment; forming a signature representing the monitored broadcast segment; comparing the signature representing the monitored broadcast segment with each of a plurality of broadcast segment signatures of the database to determine whether a match exists therebetween in accordance with a first error tolerance level; evaluating whether the match falls within a class of questionably acceptable matches based upon predetermined evaluation criteria; and, if the match falls within said class of questionably acceptable matches, comparing the signature representing the monitored broadcast segment with the matching broadcast segment signature of the database utilizing a second error tolerance level accepting matches having relatively higher error levels than matches acceptable in accordance with the first error tolerance level.

In accordance with a further aspect of the present invention, a system and method of producing a signature characterizing an audio broadcast signal for use in broadcast signal recognition, comprise the means for and the steps of, respectively, forming a plurality of frequency band values each representing portions of said audio broadcast signal within respective predetermined frequency bands; comparing each of a first group of said plurality of frequency band values with a respective one of a second group of said plurality of frequency band values representing portions of said audio broadcast signal within the same respective predetermined frequency band, each respective one of the second group of said plurality of frequency band values representing portions of said audio broadcast signal at least a part of which were broadcast prior to the portions of said audio broadcast signal represented by the corresponding one of said first group of said plurality of frequency band values; and forming said signature based upon the comparisons of the first and second groups of said plurality of frequency band values.

In accordance with still another aspect of the present invention, a system and method are provided for producing a signature characterizing an interval of a video signal representing a picture for use in broadcast segment recognition, wherein the signature is produced based on portions of the video signal representing corresponding regions of the picture each spaced a respective predetermined amount from a nominal edge of the picture, comprising the means for and the steps of, respectively, detecting a shift in the video signal corresponding with a shift in the edge of the picture from the nominal edge thereof; adjusting the portions of the video signal to compensate for said shift in the edge of the picture; and producing the signature based on the adjusted portions of the video signal.

In accordance with a still further aspect of the present invention, a system and method are provided for producing signatures characterizing respective intervals of a broadcast signal exhibiting correlation between at least some of said respective intervals for use in broadcast segment recognition, comprising the means for and the steps of, respectively, producing a difference vector for each respective interval of said broadcast signal having a plurality of elements each representing differences between respective predetermined portions of said each respective interval and exhibiting correlation therebetween; carrying out a vector transformation of said difference vector of each respective interval to produce a transformed difference vector having a plurality of elements for each respective interval of said broadcast signal such that correlation between the plurality of elements thereof is less than the correlation between the plurality of elements of said difference vector; and producing a signature for each respective interval of said broadcast signal based on the corresponding transformed difference vector.

In accordance with yet still another aspect of the present invention, a system and method are provided for producing a signature characterizing an interval of a video signal representing a picture for use in broadcast segment recognition, wherein the signature is produced based on portions of the video signal representing corresponding regions of the picture, and for producing a corresponding mask word including a plurality of bit values each representing a reliability of a corresponding value of the signature, comprising the means for and the steps of, respectively, forming a first signature having a plurality of values each based on respective ones of said portions of the video signal; forming a second signature having a plurality of values each based on respective ones of a plurality of shifted portions of the video signal each corresponding to a respective one of said portions and having a location displaced from a location of said respective one of said portions by a predetermined amount, such that each value of said first signature corresponds to a value of the second signature; comparing respective values of said first and second signatures; establishing said bit values of said mask word based on the comparison of a respective value of said first signature with the corresponding value of the second signature.

In accordance with another aspect of the present invention, a system and method are provided for updating a broadcast segment recognition database storing signatures for use in recognizing broadcast segments of interest, comprising the means for and the steps of, respectively, monitoring a broadcast signal to detect predetermined signal events indicating possible broadcast segments of interest corresponding with respective monitored broadcast signal intervals; determining whether at least two alternative possible broadcast segments of interest are detected for a monitored broadcast signal interval; assigning priority to one of said at least two alternative possible broadcast segments of interest based upon predetermined criteria; and storing a signature in the database corresponding with the one of said at least two alternative possible broadcast segments of interest assigned priority.

In accordance with a further aspect of the present invention, a system and method are provided for updating a broadcast segment recognition database storing signatures for use in recognizing broadcast segments of interest, comprising the means for and the steps of, respectively, monitoring a broadcast signal to detect predetermined signal events indicating possible broadcast segments of interest corresponding with respective monitored broadcast signal intervals; determining the extent to which the respective monitored broadcast signal intervals deviate from predetermined broadcast signal intervals of possible broadcast segments of interest; selecting ones of said respective monitored broadcast signal intervals as new segments of interest based upon the determined extent of deviation thereof from said standard lengths of broadcast segments of interest; and storing a signature in the database corresponding with the selected ones of the respective monitored broadcast signal intervals.

In accordance with still another aspect of the present invention, a system and method are provided for selectively capturing at least one of a broadcast audio signal and a broadcast video signal for use in updating a broadcast segment recognition database storing signatures for use in recognizing broadcast segments of interest, comprising the means for and the steps of, respectively, temporarily storing at least one of a broadcast audio signal and a broadcast video signal of a monitored broadcast; detecting predetermined signal events indicating possible new broadcast segments of interest of the monitored broadcast; selecting intervals of the monitored broadcast as possible new broadcast segments of interest based upon said predetermined signal events; assigning a first capture level to a first selected interval based on predetermined characteristics thereof indicating that said first selected interval is likely to be a new segment of interest; assigning a second capture level to a second selected interval based on predetermined characteristics thereof indicating that the second selected interval is relatively less likely than the first selected interval to be a new segment of interest; storing a signature corresponding with the first selected interval in the database and capturing at least one of the temporarily stored broadcast audio and video signals corresponding with the first selected interval for transmission to a workstation operator for segment identification; storing a signature corresponding with the second selected interval in the database; and erasing the temporarily stored one of the broadcast audio and video signals corresponding with the second selected interval.

In accordance with a still further aspect of the present invention, a system and method are provided for producing a signature characterizing a broadcast signal interval for use in broadcast segment recognition having a signature database, the signature including a plurality of digital words each characterizing a respective sub-interval of said broadcast signal interval, comprising the means for and the steps of, respectively, dividing the broadcast signal interval into a plurality of sub-intervals; forming a plurality of digital words characterizing each of said plurality of sub-intervals; and selecting at least one of the plurality of digital words characterizing each sub-interval based on at least one of the following factors: (a) a distribution of previously generated digital words characterizing broadcast signals; (b) a distribution of digital words of previously generated signatures

stored in the signature database; (c) a probability that the at least one of the plurality of digital words will match a digital word characterizing a corresponding sub-interval upon rebroadcast of the sub-interval; and (d) a degree of signal difference between the sub-interval corresponding with the at least one of the plurality of digital words and adjacent portions of the broadcast signal interval.

In accordance with yet another aspect of the present invention, a system and method are provided for broadcast segment recognition, comprising the means for and the steps of, respectively, producing a signature for each of a plurality of broadcast segments to be recognized; for each produced signature, determining a probability that such produced signature will match with a signature produced upon rebroadcast of the corresponding broadcast segment and producing a corresponding probability based criterion for use in evaluating a match of the produced signature; storing each produced signature and its corresponding probability based criterion to form a database; monitoring a broadcast segment; forming a signature representing the monitored broadcast segment; comparing the signature representing the monitored broadcast segment with at least one signature stored in the data base to determine a match thereof; and determining whether to accept said match based on the corresponding probability based criterion.

In accordance with a yet still further aspect of the present invention, a system and method are provided for broadcast segment recognition, comprising the means for and the steps of, respectively, producing a digital signature for each of a plurality of broadcast segments to be recognized, each said digital signature including a plurality of bit values characterizing a corresponding one of said plurality of broadcast segments; for each produced digital signature, determining a probable number of bit values thereof that will match with the bit values of a digital signature produced upon rebroadcast of the corresponding broadcast segment and producing a corresponding probability based match value for use in determining whether said each produced digital signature matches a digital signature of a subsequently received broadcast segment; storing each produced signature and its corresponding probability based match value to form a database; monitoring a broadcast segment; forming a digital signature having a plurality of bit values representing the monitored broadcast segment; comparing the digital signature representing the monitored broadcast segment with at least one digital signature stored in the database; and determining whether the digital signature representing the monitored broadcast segment matches the at least one digital signature utilizing the corresponding probability based match value.

In accordance with yet still another aspect of the present invention, a system and method are provided for broadcast segment recognition, comprising the means for and the steps of, respectively, producing a signature for each of plurality of broadcast segments to be recognized; for each produced signature, determining a probability that such produced signature will match with a signature produced upon rebroadcast of the corresponding broadcast segment; producing a further signature for said each of a plurality of broadcast segments to be recognized when said probability that said produced signature will match with a signature produced upon rebroadcast of the corresponding broadcast segment is less than a predetermined value; storing each produced signature to form a database; monitoring a broadcast segment; forming a signature representing the monitored broadcast segment; and comparing the signature representing the monitored broadcast segment with at least one signature stored in the database.

Other objects, features and advantages of the present invention will become apparent from the following detailed description of the illustrative embodiments when read in conjunction with the accompanying drawings in which corresponding components are identified by the same reference numerals.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** illustrates a system for monitoring a continuous stream of broadcast signals;

FIG. **2** is a diagram of one of the local sites in the system shown in FIG. **1**;

FIG. **3** is a diagram illustrating signal flows in the local site of FIG. **2** during a matching operation;

FIG. **4** is a diagram used to explain a method for forming a video frame signature;

FIG. **5A** and **5B** illustrate a portion of a video frame having a normal edge condition and a shifted edge condition, respectively,

FIG. **6** is a diagram to which reference is made in explaining an anti-jitter masking technique;

FIGS. **7A** and **7B** are block diagrams illustrating an audio signature generation system;

FIG. **8** is a diagram to which reference is made in explaining the operation of the audio signature generation assembly of FIGS. **7A** and **7B**;

FIG. **9** is a flow chart for explaining an occurrence filtering technique;

FIG. **10** is a diagram for explaining a confirmation matching technique;

FIG. **11** is a diagram illustrating signal flows in the local site of FIG. **2** when detecting a new segment of interest;

FIG. **12** illustrates a sequence of steps performed in detecting new segments of interest in accordance with a first operational mode;

FIG. **13** illustrates a sequence of steps performed in detecting new segments of interest in accordance with a second operational mode;

FIG. **14** illustrates a sequence of steps performed in detecting new segments of interest in accordance with a third operational mode;

FIG. **15** is a tree diagram used for describing the process illustrated in FIG. **14**;

FIG. **16** is a diagram illustrating signal flows in the local site of FIG. **2** during capture of audio and video data;

FIG. **17** is a diagram illustrating signal flows in the local site of FIG. **2** during the generation of key signatures; and

FIG. **18** is a flow chart illustrating steps performed in generating key signatures.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG. **1** illustrates a system **10** for monitoring a continuous stream of television broadcast signals and providing recognition information to which the embodiments of the present invention may be applied. As shown therein, system **10** generally comprises a central site **12**, one or more workstations **14** located at the central site **12**, and one or more local sites **16**. Each of the local sites **16** monitors broadcasting in a corresponding geographic region.

The central site **12** communicates with each of the local sites **16**, for example, via telephone lines, to receive data regarding detection of known broadcast segments and potentially new, unknown segments, and to provide segment signature and detection information corresponding to new broadcast segments. The central site **12** compiles the received data and formulates the same into a report **13** which, for example, may be supplied to broadcast advertisers.

The central site **12** also supplies broadcast data, for example, audio and video data, to the workstations **14** where new and unknown segments are identified by human operators and assigned an identification code. If a site identifies a portion of a broadcast as a new segment of interest (such as a commercial), when it is in fact something else (such as normal programming), workstation operator time to identify the unwanted segment is wasted. Also, if an already known segment cannot be correctly identified by the system **10**, it may be reported incorrectly by the central site **12** to a workstation **14** as a new segment, thus further wasting operator time. The cost to employ operators is a significant ongoing expense. Accordingly, it is desirable to minimize this expense by accurately detecting new segments of interest and identifying known segments. The present invention provides improved methods and apparatus for signal recognition which achieve an enhanced ability to accurately identify known segments of interest as well as minimization of the need to identify potentially new segments with the assistance of workstation operators. In accordance with the disclosed embodiments of the invention such improved methods and apparatus are implemented at the local sites **16** of the system **10**.

Each local site **16** is adapted to receive an RF broadcast signal from, for example, an antenna **18** or a cable television head end station (not shown for purposed of simplicity and clarity) and is capable of recognizing and identifying known broadcast segments by date, time, duration, channel, and other desirable information. The local sites **16** are also capable of recognizing the occurrence of potentially new, unknown segments, and of generating temporary key signatures therefor so that it can maintain a record of such occurrences pending identification of the segment by a workstation operator at the central site. Although the system **10** only illustrates three local sites **16**, the system is not so limited and any number of local sites may be utilized. Similarly, the system **10** is not limited to only two workstations **14** as shown in FIG. **1**.

FIG. **2** illustrates one of the local sites **16** in block form. As shown therein, each local site **16** generally comprises a front end portion **20** and a back end portion **22**. The front end portion **20** includes one or more RF broadcast converters **24**, a segment recognition subsystem **26**, a sensor **27** and a data capture subsystem **28**. The back end portion **22** includes a control computer **30** and at least one disk drive **32**.

Each of the RF broadcast converters **24** receives television broadcast signals over a respective channel and demodulates the received signals to provide baseband video and audio signals. The video and audio signals are thereafter supplied to the segment recognition subsystem **26**, wherein frame signatures for each of the video and audio signals are generated which are thereafter compared to stored key signatures to determine if a match exists. For purposes of clarity, video and audio signatures are separately termed "subsignatures" herein. The segment recognition subsystem also produces cues which represent signal events, such as a video fade-to-black or an audio mute. The cues as well as match information are supplied to the control computer **30** for use in determining whether the received signal represents a new segment or commercial of interest, determining whether to capture video and audio information for use at the central site in identifying a new segment of interest, assessing the validity of questionable matches, and for grouping match information for storage in a database.

The sensor **27** is adapted to monitor the operating temperature of the front end **20** and, in the event that the operating temperature exceeds a predetermined maximum operating temperature, to supply a signal so indicating to control computer **30**. More specifically, sensor **27** receives temperature information relating to the subsystems **26** and **28** from one or more thermocouples **29** and processes such received temperature information for supply to the computer **30**, so that if excessive temperatures are encountered, the subsystems **26** and **28** are turned off.

The data capture subsystem **28** receives the broadcast audio and video signals from the converters **24** by way of the segment recognition subsystem **26** and compresses and digitizes the same. These digitized signals are stored in a buffer contained within the subsystem **28** for a predetermined time period, and upon request are supplied to the control computer **30**.

The control computer **30** is adapted to select key signatures, provide match confirmation, process new segment data and communicate with the central site **12**. The disk drive **32** provides mass data storage capability for match occurrence information, new commercial information and audio/video data for transmission to the central site **12**.

FIG. **3** illustrates the data flow for a typical matching operation. As shown therein, one of the converters **24** receives a desired channel of broadcast signals which are supplied as baseband video and audio signals to the segment recognition subsystem **26**. The subsystem **26** includes a plurality of channel boards **402**, one for each channel monitored by the local site **16**, which each serves to generate a corresponding frame subsignature and mask word for each frame of the baseband video signal. In addition, each channel board generates a frame subsignature and mask word for each interval of the audio signal corresponding with a frame of the video signal and having the same format as the video subsignatures and mask words. It is appreciated that the use of corresponding intervals and data formats for the video and audio subsignatures advantageously facilitates processing thereof. It is also appreciated that subsignatures may be produced from different intervals, such as video fields or combinations of fields or frames or otherwise, and that the video and audio subsignatures and mask words need not follow the same format. The channel boards **402** also serve to detect video signal fades-to-black based on the receipt of at least one substantially black field or frame of the received baseband video signal, as well as audio mutes, a reduction of the baseband audio signal level representing silence. The channel boards **402** also serve to detect video scene changes indicated by a rapid change in the video signal. These signaling events, as well as the video and audio subsignatures and mask words, produced by the channel board **402** are received by the segment recognition controller **404**. Each local site **16** is provided with at least one auxiliary converter **24** and channel board **402**, so that if one of the converters **24** and channel boards **402** should fail to operate, the segment recognition controller **404** generates a command to an auxiliary channel board and converter which then assume the functions of the inoperative equipment.

The segment recognition controller **404** communicates with a segment signature ring buffer **406** to store newly

received segment signatures, that is, sequentially arranged frame signatures and mask words for each channel, for a predetermined time interval preceding the current time. The segment recognition controller also communicates with a correlator **420** to supply match commands thereto. The correlator **420** is also supplied with the appropriate segment signatures from the segment signature ring buffer **406** and key signatures from a key signature database **408**. The correlator **420** performs the requested matching operation and supplies the match results, along with the relevant information (e.g., the corresponding error count), to the segment recognition controller **404**. The segment recognition controller **404** supplies a match report for each audio and video subsignature and signalling events to an expert system module **414** implemented by the control computer **30**.

The expert system **414** evaluates each received match report to decide whether it is erroneous. In certain situations, the expert system **414** utilizes a configuration matching process in the match report evaluation. In that event, the expert system supplies a confirmation match request to a confirmation matching module **422** also implemented by computer **30** which, in response thereto, supplies a signal to the segment recognition controller **404** requesting the appropriate segment signature. In response to such a request, the segment recognition controller supplies the appropriate segment signature to the confirmation matching module **422**. In addition, the confirmation matching module receives the appropriate key signature from a database **412** maintained by a database control module **416** of the computer **30** under the control of the expert system **414**. Upon completing the confirmation matching process, the confirmation matching module **422** supplies a confirmation match signal to the expert system **414**. In response thereto, the expert system **414** supplies matching information, for example, occurrence data, through the database control module **416** to the database **412**.

In certain situations, the expert system **414** may supply occurrence data prior to receiving the confirmation match response. If, in these situations, the confirmation matching module **422** determines that an acceptable match does not exist, the expert system **414** supplies a match rescind signal through the database control **416** to the database **412** whereupon the previously supplied occurrence is rescinded.

VIDEO SIGNATURE GENERATION

Each of the channel boards **402** produces video frame signatures by first producing a difference vector **150** in the form of an ordered sequence of elements $x_1, x_2, \ldots, x_{16}$ for each video frame in accordance with the technique illustrated in FIG. **4**. As shown in FIG. **4**, a frame **140** of a video signal includes a back porch region **141**, a picture region **142** and a front porch region **143**. The left edge **146** of the picture region **142** is bounded by the right edge of the back porch region **141**, whereas the right edge **147** of the picture region **142** is bounded by the left edge of the front porch region **143**.

Thirty-two predetermined superpixel areas **144** are defined for each frame, of which sixteen exemplary superpixel areas are illustrated in FIG. **4**. Each superpixel area **144** is rectangular and includes, for example, between 18 and 21 pixels in each of 4 vertically adjacent horizontal lines from the picture area **142**. A portion **144** is selected, as described in greater detail hereinafter, and an average luminance value thereof is produced. Each superpixel area **144** is paired with a respective other area **144** as indicated by the dash lines **148** in FIG. **4** for comparing the respective average luminance values thereof. Each such pair of respective average luminance values is used to produce the value of a corresponding element x_n of the difference vector **150**. For example, the average luminance value of the selected portion of superpixel area **144***a* is subtracted from that of paired superpixel area **144***b* to produce the value of a corresponding element x_n of the difference vector **150**.

Thereafter, each difference vector **150** is subjected to a sequence of vector transformations described hereinbelow which yield a corresponding sixteen-element transformed or resultant vector. Then a sixteen-bit frame signature is produced wherein each bit is either set or reset depending on the sign of a corresponding element of the resultant vector. In addition, the value of each element of the resultant vector is examined to determine whether (1) its absolute value is less than a guard band value, or (2) it is susceptible to jitter (as explained below). If either condition (1) or (2) obtains, then the corresponding mask bit of a respective 16-bit mask word is set.

Video Edge Detection

With reference again to FIG. **4**, it will be appreciated that the positions of the superpixel areas **144** must be accurately determined with respect to an edge of the picture region **142** so that pixels of each portion used for producing the respective average luminance values correspond from frame to frame. The video signals of television commercials are often received with a horizontal shift from a normal or standard position. The horizontal shift most often encountered is a shift to the right as determined by viewing a television receiver which would result in a shift to the right of the edge **146** of picture area **142** in FIG. **4**. While horizontal shifts to the left may occur, such shifts occur significantly less often than shifts to the right. Although most horizontal shifts or offsets are typically not large enough to be detectable by a viewer, these shifts may affect the generation of frame signatures by shifting the edge of each video frame's picture area **142** thereby shifting the portions of the superpixels used in signature generation. If not compensated, this effect will degrade the ability of the system **10** to reliably produce frame signatures and, thus, adversely affect system accuracy overall.

A video edge detection module, implemented by each of the channel boards **402** of FIG. **3**, is provided for detecting a shift in the edge of the picture region **142** of a received video signal. Since, as previously mentioned, horizontal shifts to the right have been observed to occur more frequently, in describing the video edge detection module, it will be assumed that a horizontal shift to the right has occurred. However, the present invention is not so limited and may be utilized for horizontal shifts to the left.

FIG. **5A** illustrates a video frame having a standard or normal edge location. As shown therein, the video frame includes a back porch portion, a picture area and a front porch portion. FIG. **5B** illustrates a video frame having a horizontal shift to the right, in which such a shift increases the size of the back porch portion and decreases the picture area by a corresponding amount.

The video edge detection module places at least one edge detection superpixel **100**, which is a rectangular sampling area, across the boundary between the picture area and the back porch area, as shown in FIGS. **5A** and **5B** so that the superpixel **100** includes the normal edge location as well as

adjacent picture regions to which the edge may be shifted. The video data from within such edge detection superpixels **100** are processed to determine the position of the left edge of the picture area. Each edge detection superpixel **100** advantageously has the same area as that of each superpixel area **104**, which preferably has a size of approximately 18 to 21 pixels in length by 4 pixels in height. As such, each edge detection superpixel **100** contains portions from more than one video line. Each of these video lines within the superpixel **100** provides data on the left picture edge position. In an advantageous embodiment, the left edge positions obtained from each line in all of the edge detection superpixel areas **100** are combined to produce an estimated location for the left edge of the picture area. By so combining all of the left edge position data, a more reliable estimate of the left edge is obtained as compared to that derived from using just a single line of edge position information which may be adversely influenced by noise in the video signal.

Thus, the left edge of the picture is obtained by combining the left edge values obtained for each of the video data lines in all of the edge detection superpixel areas **100**. In so determining the left edge of the picture, it is preferable to discard extreme values obtained from the video data lines and average the remaining values. In a preferred embodiment, the two lowest values as well as the highest value for the left edge of the picture are considered extremes and, as such, are discarded. Since signal noise is more apt to result in a low value, more low values for the left edge are discarded.

As previously mentioned, there are 32 superpixel areas **144** associated with each frame of the video signal. Within each of these superpixel areas **144** is a sampling area **102**. This sampling area **102** is the area from which the video data are extracted for use in generating the respective frame signature. For example, FIG. 5A illustrates the location of the sampling area **102** within the superpixel area **144** for a frame having a standard edge condition. When the superpixel areas **144** measure between 18 and 21 pixels by four lines, the sampling areas are selected advantageously to measure 4 pixels by 4 lines. When a horizontal shift in the left edge of the picture is detected as previously discussed, the effects of such a shift upon the sampling area **102** may be compensated by changing the sampling area **102** in accordance with the detected horizontal shift as shown in FIG. 5B. That is, if the left edge of the picture is determined to have shifted to the right by N pixels from the normal position, then the sampling area **102** is also shifted to the right by N pixels.

In a preferred embodiment, the video edge detection module preferably uses a predetermined minimum number of video data lines (e.g., approximately 6–8) from the edge detection superpixel areas **100** to locate the left edge of the picture area. However, when the portion of the picture area adjacent to the back porch is relatively dark, it may be difficult to accurately locate the left edge of the picture area from any of the lines of video data contained within all of the edge detection superpixel areas **100**. In this situation, a predetermined default value is used for the left edge of the picture area.

If the horizontal offset extends beyond the edge detection superpixel areas **100** such that the left edge of the picture lies outside the areas **100**, then the video edge detection module considers the left edge not to have been found. In this situation, the above mentioned predetermined default value is used. Furthermore, in some instances, a horizontal offset may be detected which is larger than can be compensated for, that is, the sampling area **102** cannot be shifted an amount corresponding to the horizontal offset. In this situation, the sampling area **102** is shifted the maximum amount possible.

To determine the left edge of the picture area for each video line, the video edge detection module scans the pixel samples from left to right searching for a jump or increase in the luminance value of more than a predetermined amount between a respective pixel and the pixel which is located two pixels to the right of the respective pixel. If such a jump is detected, the difference in luminance values between the pixel currently being tested and the pixel three pixels to the right is then determined to ensure that the increase in luminance value is again equal to the predetermined value to filter out noise spikes. Further, by examining pixels which are located two pixels to the right of the pixel being tested, instead of testing adjacent pixels, an edge may be detected which otherwise would be undetectable when adjacent pixels are tested. That is, in relatively dark video scenes, the slope (difference) of the edge picture values is less than in relatively bright scenes.

The video edge detection module may place the left edge of the picture one or two pixels before the edge actually occurs. This does not present a problem as the video edge detection module corrects for differences between left edge positions for different broadcasts and need not detect an absolute edge position.

Thus, the video edge detection module enhances system accuracy by enabling reliable video frame signatures to be obtained from the received video signal. Further, the video edge detection module compensates for the horizontal offsets without requiring any additional hardware at the local site **16**.

Video Preprocessing

It has been observed that certain values of video frame signatures occur more often than other values of video frame signatures so that video frame signatures tend to become concentrated together at certain values (sometimes referred to as "clumping" herein). Such clumping of video frame signatures may present several problems. First, a frequently occurring video frame signature, termed a "clump signature", is likely to be selected as a keyword. As a result, this keyword or clump signature may have a large number of key signatures associated with it. Since the correlator **420** of the segment recognition system **26** searches all key signatures corresponding to a respective keyword, clumping signatures can greatly increase the processing time of the correlator. As a result, this may limit the amount of data which may be stored within the database of the local site **16** and/or the number of broadcast channels which may be processed. Secondly, clumping may cause an increase in false matching. That is, as the number of signatures which are associated with a clump signature keyword increases, the closer the bit patterns of these signatures may come to one another. As a result, if a slight change in a segment signature occurs, for example, due to signal noise or jitter, the correlator **420** may inaccurately report a match.

Clumping can be considered to cause a reduction in the actual amount of information in a signature. For example, in the situation wherein all of the video frame signatures are the same, the value of each signature is known in advance. Therefore, in this situation, the value of the next video frame signature may be described by zero bits. At the other extreme, that is, when the video frame signatures are completely random so as to have a uniform distribution of

values, all of the bits within the signature are needed to identify the respective signature.

Such clumping may be reduced or minimized by increasing the uniformity of the video frame signature distribution. For example, if the video frame signatures were uniformly distributed, each signature would occur with equal frequency. Each of the channel boards **402** of the segment recognition subsystem **26** (FIG. **15**) preprocesses the input video signal to produce video frame signatures which are more uniformly distributed. That is, channel board **402** transforms the input video signal by utilizing a vector transform which, in turn, utilizes statistical data pertaining to relevant clumping information to reduce or minimize clumping of video frame signatures by reducing the correlation between the bits of each frame, which results in a more uniform distribution of signatures. The vector transform processing performed by the channel boards **402** will now be described in more detail.

In an advantageous embodiment of the invention, a Hotelling transform is employed to carry out a vector transformation of the difference vector **150** FIG. 4 which is designated x hereinbelow and includes sixteen ordered elements ($x_1, x_2, \ldots, x_{16}$), which results in a reduction of the covariance between the elements $x_1, x_2, \ldots, x_{16}$ of x. The Hotelling transform may be expressed as follows:

$$y=A(x-m)$$

in which x represents the difference vector **150**, m is a vector which represents the mean values of the elements of x, A represents a transformation matrix and y is a vector which represents the transformed vector x. Once the transformed vector y has been produced, a frame signature is obtained therefrom by converting the sign of each element of the vector y into a respective bit value of the frame signature. That is, positive elements of the vector y are assigned one binary value, while negative elements thereof are assigned the other binary value. Each element in the transformed vector y may be expressed as follows:

$$y(i)=\Sigma[A(i,j)*(x(j)-M(j))],\ J=1 \text{ to } 15$$

The covariance of y may be expressed as follows:

$$\begin{aligned}[C_y] &= yy' \\ &= [A(x-m)]\,[A(x-m)]' \\ &= A(x-m)\,(x-m)'A' \\ &= A(C_x)\,A'\end{aligned}$$

which (') represents the transpose of the respective vector. If the rows in the matrix A are selected as the normalized eigenvectors of the matrix C_x (the covariance of x), the C_y matrix is diagonal. As a result of such selection, the bits of the newly formed frame signature (FIG. **10**), which are derived from y, are uncorrelated. However, although the bits contained within the frame signature are uncorrelated, they may not be statistically independent. Nevertheless, their interdependence with one another is reduced. In a preferred embodiment of the present invention, the transformation matrix A is assumed to be a constant. This assumption implies that the incoming video signal is a wide-sense stationary process so that the values for C_x and m are constant.

T determine the value of the transformation matrix A, the values for the vectors m and $[C_x]$ are utilized. These values may be obtained as follows:

$$m=(1/N)\,\Sigma(x),\ j=1 \text{ to } N \tag{4}$$

and

$$[C_x]=\left[\ (1/N)\sum_{j=1}^{j=N}(xx')\ \right]-mm' \tag{5}$$

in which N represents the number of samples of x which are employed to determine the values of m and $[C_x]$. Upon determining the value of $[C_x]$, the transformation matrix A may be obtained by determining the eigenvectors of $[C_x]$.

To minimize susceptibility to frame jitter, the frame signature is calculated a predetermined number of times and the obtained signatures compared for differences therebetween. That is, in a preferred embodiment, the frame signature is determined as if horizontal shifts in the associated video frame of −1, 0 and +1 pixels have occurred. If a bit or bits in these three signature words vary from one to another, then the corresponding mask bit or bits are set. Further, if a transformed difference value is relatively close to zero, the mask bit corresponding thereto is set.

If the Hotelling transformation process is applied to a video signal as described above, relatively large clump signatures may not be broken up as finely as desired. That is, since the covariance used in this process is based on video data from all of the input video frames, whereas the frames having clumped signatures account for only a relatively small percentage of all of the frames, the effective contribution of the frames having clumped signatures to the covariance may be small. One approach to more effectively breakup these relatively large concentrations of frame signatures is to utilize separate transformations for groups of frames having similar signature values and occurring with greater than average frequency which are referred to hereinafter as "clumps". Such a transformation will also effectively breakup clumps associated with signatures having values which are bit-opposites of those associated with the original clump.

Using a single transformation process increases the uniformity of the frame signature distribution and, as a result, the number of video frames associated with respective frame signature values are closer to the average number of frame signatures obtained by utilizing the transformation process and have a higher acceptable match rate associated therewith as compared to signatures obtained without transformation.

On the other hand, the use of different transformations for different signature values or ranges of signature values can increase the uniformity of the frame signature distribution even over that obtained using a single transformation. More specifically, when using such multiple transformations, incoming signature words are categorized as either belonging to a clump or not belonging to a clump, that is, a concentration of frame signature occurrences (or greater frequency of occurrences) at a certain signature value or range of values. This categorization is performed by determining the distance, for example, the Hamming distance, of an incoming frame signature from a model template. Hamming distance refers to the number of bits which are different between two binary words and the model template contains the frame signature or signatures which represent the center of a clump. If the incoming frame signature lies within a predetermined Hamming distance or number of bits from the model template frame signatures, the respective signature is transformed using an appropriate one of the plurality of the transformations. A Hamming distance of either one or two bits from the model template provides an improved signature distribution, with a distance of two bits being preferred.

When a received frame would produce a signature which has a value lying on the border of values produced by

ADOBE – Exhibit 1002, page 194

JAFFE-ADOBE000228

different transformations, it is important that the transformation employed yield a signature which will match that of the same frame if subsequently received. To avoid sensitivities to the influence of noise which might result in the production of different signatures for the same frame received at different times, in such borderline cases frame signatures are produced by using both transformations whereupon mask bits are set in each corresponding mask word for any corresponding bits in the signatures produced by the different transformations which differ from one another. Accordingly, by carrying out a vector transformation of a difference vector representing the information content of a frame, it is possible to reduce correlation between the elements thereof thereby improving the evenness of the distribution of frame signatures which otherwise would become concentrated about certain values. A particularly advantageous technique employs a Hotelling transform to reduce the covariance between the vector elements, such that their correlation is thereby reduced.

Anti-Jitter Masking

An anti-jitter masking module is implemented by each of the channel boards **402** and is adapted for making the video frame signatures less sensitive to horizontal and vertical shifts in the video picture which may vary from broadcast to broadcast. Such horizontal and vertical shifts may be due to hardware timing instabilities or to instability in the transmitted video signal.

More specifically, the anti-jitter masking module compensates for both short term horizontal and vertical shifts known as jitter and/or systematic offsets which may be caused by the transmitting hardware or by the receiving hardware. As is appreciated, the systematic offsets may also be compensated by the edge detection module, as previously described.

As described above, both a 16-bit signature word and the corresponding 16-bit mask word are generated for each video frame. Each bit in the mask word corresponds to a bit in the signature word. By setting a bit in the mask word, portions of system **10** (FIG. **1**) which utilize the video frame signature are effectively warned that the corresponding bit in the video frame signature should be considered unreliable. For example, this warning is used in selecting the keyword and matchwords for a key signature and in setting the error threshold for finding a match using a given key signature. Further, since errors which occur on bits in a frame signature word which correspond to bits set in the mask word are expected, this warning is also utilized in the correlator **420** of the segment recognition sub-system **26** to determine error counts in the matching process.

The anti-jitter masking module produces respective sums of pixel luminance values for each superpixel area and a predetermined number (for example, four) of adjacent superpixel areas. In an advantageous embodiment, the adjacent superpixel areas include an area which is shifted up and to the left of the respective superpixel area, an area which shifted up and to the right of the respective superpixel area, an area which is shifted down and to the left of the respective superpixel area, and an area which is shifted down and to the right of the respective superpixel area. From each of these five superpixel areas, that is, the respective superpixel area and the four shifted superpixel areas, respective sums of the luminance values of the pixels contained within the areas are produced. Similar values are obtained for the other **31** superpixel areas contained within each video frame to produce four sets of thirty-two values each for a corresponding shifted group of superpixel areas. Afterwards, five video frame signatures are generated, that is, one by utilizing the 32 unshifted superpixels and four by utilizing each of the four sets of 32 shifted superpixels. FIG. **6** illustrates this exemplary process carried out for one superpixel. In FIG. **6**, a main superpixel **120**, which has a size of four pixels wide by four pixels high, is shifted in the above-described manner by two pixels in the vertical and two pixels in the horizontal direction. That is, a superpixel area **122** is located by shifting a sampling area two pixels up and two pixels to the left from the main superpixel **120**. Similarly, superpixel areas **124**,**126** and **128** are also obtained by shifting a sampling area by two pixels down and to the left, by two pixels down and to the right and by two pixels up and to the right.

If any bit in the video frame signatures corresponding to the four shifted superpixel areas differs from that in the video frame signature obtained from the unshifted (main) superpixel area, then that bit is considered to be sensitive to jitter whereupon the mask bit which corresponds to this bit is set. It is appreciated that, by so examining each of these respective superpixel areas, the anti-jitter masking module determines whether the value of a particular bit contained within the video frame signature word would change if there was a shift in the video picture which corresponds to the shift used to obtain the shifted superpixel.

The amount by which the superpixel **120** of FIG. **6** is shifted in the vertical and horizontal directions may be varied. To some extent, the greater the shift in the vertical and horizontal directions of the superpixel **120**, the larger the shift in the vertical and horizontal direction of the video signal which can be compensated by the anti-jitter module. However, a relatively large shift of the main superpixel area **120** in the vertical and/or horizontal directions may result in a relatively large number of bits being set in the mask bit word. It is appreciated that, if too large a number of bits is set in a mask word, the corresponding frame signature word contains almost meaningless information. For example, if the main superpixel **120** is shifted a relatively large amount in the horizontal and/or vertical directions, the results obtained therefrom would indicate that most if not all of the bits are sensitive to jitter. As previously described, in one embodiment of the present invention, each main superpixel **120** is shifted two pixels in the horizontal direction and two pixels in the vertical direction. In another advantageous embodiment of the present invention, each superpixel **120** is shifted one pixel to the right and to the left in the horizontal direction but without a vertical shift.

Thus, the anti-jitter masking module sets bits within the mask bit word for corresponding bits contained within each video frame signature which may be sensitive to jitter or offsets. Further, the anti-jitter masking module, like the edge detection module, is primarily included in a software program of the segment recognition sub-system **26** and, as such, requires minimal cost to implement in each of the local sites **16**.

The anti-jitter masking technique is preferably carried out in combination with a guard band masking technique in which the mask bit for a given frame signature bit is masked if the absolute value of the difference between the average luminance values of the two corresponding superpixel areas is less than a predetermined guard band value. For example, if luminance values for a given video signal are digitized within a scale of zero to 256, an exemplary guard band value of 64 may be selected. If the mask bit of a corresponding vector element is set, the mask bit of the respective signature bit is set. That is, the mask bit of any given signature bit is

set if either guard band masking or anti-jitter masking sets such mask bit.

AUDIO SIGNATURE GENERATION

With reference to FIG. 7A, audio signatures are generated by an audio signature generation assembly **250** illustrated therein incorporated in each of the channel boards **402** (FIG. 3) for each broadcast channel of audio data which is to be monitored. The audio signature generation assembly **250** generally comprises an audio signal conditioning and sampling circuit **202**, an A/D conversion and input buffer circuit **204**, a transformation and signature extraction module **206** and an output circuit **208**. More specifically, a baseband audio signal from one broadcast channel is supplied to the circuit **202**. In a preferred embodiment, the audio baseband signal is low pass filtered by the circuit **202** to satisfy the Nyquist criterion and to emphasize voice signal content over music and other sounds, which simplifies processing and memory requirements without sacrificing needed informational content, since the overwhelming majority of television audio signals contain human speech. The band limited signal from the circuit **202** is supplied to the circuit **204** for conversion into digital form. The digitized audio from the circuit **204** is supplied to the transformation and signature extraction module **206** which utilizes a Fast Fourier Transform process (FFT) for generating audio frame signatures and corresponding mask words. The audio signatures and mask words are supplied to the output circuit **208** for conversion to a form suitable for output from the segment recognition subsystem **26**. The audio signature generation assembly **250** is shown in more detail in FIG. 7B which will now be described.

As shown in FIG. 7B, the audio signature generation assembly **250** includes an analog portion (which contains the audio signal conditioning and sampling circuit **202**) and a digital portion (which contains circuits **204** and **208** and module **206**). The circuit **202** comprises an automatic gain control (AGC) circuit **254**, a switched-capacitor filter **256** and a sample and hold circuit **258**. More specifically, a baseband audio signal from one broadcast channel is supplied to the automatic gain control (AGC) circuit **254** to maintain a relatively uniform audio power level. That is, since the Fast Fourier Transform (FFT) processing accumulates audio power during normal processing, it is desirable to prevent the audio input power from becoming relatively large to avoid clipping of the output FFT processed signal. An output signal from the AGC circuit **254** is supplied to the switched-capacitor filter **256** which, in a preferred embodiment, is a lowpass filter having a 3 dB roll-off at a frequency of approximately 3200 Hz, since the power density spectrum for speech falls off rapidly at frequencies above 3 kHz. The output signal from the switched-capacitor filter **256** is supplied for audio signal capture (described hereinbelow) and is further supplied through the sample and hold circuit **258** to the A/D conversion and input buffer circuit **204**. It is appreciated that in the alternative, unfiltered audio signals may be supplied for audio signal capture.

The circuit **204** comprises an analog-to-digital converter **260** and a first-in-first-out (FIFO) buffer **262**. The output signal from the sample and hold circuit **258** is supplied to the analog-to-digital converter **260** which receives a timing or sampling signal, which is derived from a video horizontal synchronization pulse signal, from a timing circuit **266**. In a preferred embodiment, the sampling signal has a frequency of approximately 15,260 Hz. As a result, the converter **260** samples the received audio data with a sampling rate of approximately 15,260 Hz. The output from the converter **260** is supplied to the FIFO buffer circuit **262**. The output from the FIFO circuit **262** is supplied to an audio digital signal processor **264** included in the transformation and signature extraction module **206**. The digital signal processor **264** serves to process the received audio data to create audio signatures and corresponding mask signatures whose data format and timing corresponds with that of the video frame signatures and mask words for simplification of further processing. Timing signals for the digital signal processor **264** are supplied from the timing circuit **266**. The output signal from the digital signal processor **264**, which includes the audio signatures and the corresponding mask words, is supplied to the output circuit **208**.

The output circuit **208** comprises a first-in-first-out (FIFO) buffer circuit **268**, a microprocessor **270**, a dual port RAM **272** and an interface circuit **274**. The output signal from the digital signal processor **264** is supplied through the first-in-first-out (FIFO) buffer **268** to the microprocessor **270**. Since the processing rates associated with the digital signal processor **264** and the microprocessor **270** may differ, the FIFO circuit **268** buffers the data from the digital signal processor for supply to the microprocessor. The microprocessor **270**, which may be an Intel **80188**, serves to extract the audio signature and mask word data received from the FIFO circuit **268** at predetermined intervals. This extracted data is thereafter supplied through the dual port RAM circuit **272** to the interface circuit **274**. Since the output data signal from the Intel 80188 microprocessor **270** has an 8-bit format while the interface circuit **274** is designed to transfer data signals having a 16-bit format, the dual port RAM circuit **272** buffers the received 8-bit data to output 16-bit data therefrom.

The processing performed by the digital signal processor **264** in creating the audio signatures and the corresponding mask signatures will now be described more fully.

The processing performed by the digital signal processor **264** is synchronized to the corresponding video fields such that a complete processing sequence is repeated every video frame. More specifically, the digital signal processor **264** transforms 256 words of audio data received from the FIFO circuit **262** into 128 complex data points by averaging adjacent ones of the **256** words and by setting the imaginary words to zero. This reduces the data rate to approximately 7.6K digital samples/second. It will be appreciated that the input data rate for FFT processing satisfies the minimum sampling frequency requirement so that aliasing is avoided. A 50% overlap in the Fast Fourier Transform is obtained by using the 128 complex data points which were generated for the previous field along with the new **128** complex data points for the current field. This data overlap has the effect of allowing fair contribution of all the data points within the window including the boundary points.

With reference to FIG. **8**, which generally illustrates the sequence of processing steps carried out by the processor **264** the above complex data points are generated by an input module **300** and thereafter a window module **302** multiplies the complex data points by window coefficients, which in a preferred embodiment effects a Hanning or cosine squared windowing process. In such cosine squared windowing, the amplitude of an audio signal sample is multiplied by a factor which is proportional to the square of the cosine of an angle which corresponds with a location in time of the respective sample within the corresponding frame interval. Such multiplication reduces the presence of signal spikes at either end of the frame interval and injects a degree of periodicity into the audio data signal to improve the results of the FFT

processing. More specifically, since Fast Fourier Transform processing is primarily designed for use with periodic signals, if the signal being transformed is not substantially periodic, the transformed signal may be incorrectly spread across several frequency bands. Processing the complex data points with window coefficients, such as those associated with a cosine squared window, minimizes the tendency for such signal spreading. The previously described data averaging process and overlapping process, together with the cosine squared windowing process, provides a processing base which minimizes frame-to-frame timing differences in the received audio signal and permits equal frequency contributions to each portion of the audio spectrum of interest.

The multiplied data produced by the window module **302** are processed by an FFT module **304** which performs a 256 complex point radix-2 DIF (decimation in frequency) transform using the appropriate weighting or twiddle factors, which may be stored in a look-up table which is downloaded to the digital signal processor **264** from the control computer **30** (FIG. 2) during a start-up protocol. The FFT module **304** effectively implements 256 different bandpass filters. The output produced the FFT module **304**, which represents both magnitude and phase information of the audio signal in each band, is supplied to a magnitude squared module **306** to obtain a power or magnitude-squared value for each of the bands within the frequency spectrum. As a result, the phase information from the FFT module **304**, which is not needed in subsequent processing, is effectively discarded by the module **306** and is not supplied therefrom.

The magnitude squared module **306** produces magnitude squared values representing the power of the complex spectral points output by the FFT module **304**. Due to symmetry, only the first half of the power spectrum is calculated. The result of the square operation is a 30-bit number plus 2 sign bits, of which only 16 bits are saved. Generally, the values are small, so that a saturation scaling process is employed whereby the upper 16 bits are saved after shifting each data word left by a predetermined number of bit places (for example, 6 bit places). If the shift causes an overflow, the resulting word is set to a saturation value of FFFF (Hex).

The values produced by the magnitude-squared module **306** are processed by a band selection module **308** to select frequency band values for a predetermined number of bands. The band selection is performed in accordance with predetermined instructions stored in a look-up table which is downloaded to the digital signal processor **264** during the start- up protocol. In a preferred embodiment, the frequency band values of 16 bands are selected and processed by a finite impulse response (FIR) filter module **310**. The FIR filter **310** performs a 15-stage finite impulse response filter operation on each of the received 16 frequency band values. Coefficients for the FIR filter **310**, which in a preferred embodiment are Hamming window coefficients selected to carry out a lowpass filtering operation, are supplied from a look-up table which is downloaded to the digital signal processor **264** during the start-up protocol.

Audio signal timing shifts with respect to the simulcast video are commonly encountered in broadcast television and, if ignored in the audio signature generation process, can result in audio signatures which are out of phase with the corresponding video signatures. This will likely degrade the ability of the system **10** to accurately match incoming segments. The FIR module **310** serves to improve signature stability by averaging the audio spectral data over a number of television frames, thus to enhance the likelihood of obtaining correct signature matches.

By averaging the frequency band values over a number of frames, the processing carried out by the module **310** also serves to maximize frame-to-frame correlation. This tends to create groups of similar signatures having a duration of several frames and referred to as runs. The presence of run lengths permits the generation of audio key signatures which are more likely to match when the same audio segment is again received by the system **10**, thus promoting system accuracy and efficiency. Another advantage is that errors resulting from noise, quantization and roundoff are less critical since these tend to be averaged out.

The filtered output signals from the FIR filter **310** are then processed by a clamping module **311** which is adapted to clamp the filtered output signals between predetermined high and low values. Clamping the filtered signals to a predetermined high value prevents overflows which may otherwise occur during subsequent processing, whereas clamping the filtered signals to a predetermined low value prevents possible division by zero and the predetermined clamping values are selected accordingly. For example, where the averaged frequency band values to be clamped are provided as 16-bit words ranging in value from 0–FFFF (Hex), a lower clamping value of F(Hex) may be employed, while an upper clamping value of 3FFF (Hex) may be employed.

The output produced by the clamping module **311** is then processed by a normalization module **313**, whereupon each of the values obtained by the clamping module are normalized in a predetermined manner. This normalization may be performed for several of the 16 clamped band values by dividing the respective value of each band by the sum of the values in the bands both above and below the respective frequency band. At the edge of the frequency spectrum, however, values from bands either above or below the edge band are utilized (or else only a single adjacent band value is employed). In other situations, however, values from three bands may be utilized in determining the normalized value for a respective band. This normalization process may be represented as follows:

$$Bn\ \text{normal} = \frac{B_n}{B_{adj}} \tag{6}$$

in which, B_n represents the clamped value for a respective band n, B_{adj} represents the clamped value(s) for the adjoining band(s). Table I below illustrates the adjoining band(s) used in determining the normalized value in accordance with a preferred embodiment. By utilizing varying numbers of bands to produce B_{adj} for different frequency bands in the normalization process, the statistical distribution of audio signatures among the keywords can be made more even. As a result, clumping of audio signatures around certain keywords is reduced.

TABLE I

Band	Center Freq.	B_{adj}
Band 1	120 Hz	BAND 2 + BAND 3
Band 2	150	BAND 1 + BAND 3 + BAND 4
Band 3	180	BAND 2 + BAND 4
Band 4	210	BAND 3 + BAND 5 + BAND 6
Band 5	240	BAND 4 + BAND 6
Band 6	300	BAND 5 + BAND 7 + BAND 8
Band 7	360	BAND 6 + BAND 8
Band 8	420	BAND 7 + BAND 9 + BAND 10
Band 9	480	BAND 7 + BAND 8 + BAND 10
Band 10	600	BAND 9 + BAND 11
Band 11	720	BAND 9 + BAND 10 + BAND 12

TABLE I-continued

Band	Center Freq.	B_{adj}
Band 12	840	BAND 11 + BAND 13
Band 13	960	BAND 11 + BAND 12 + BAND 14
Band 14	1440	BAND 13 + BAND 15
Band 15	1920	BAND 13 + BAND 14 + BAND 16
Band 16	2400	BAND 14 + BAND 15

Table I also summarizes an advantageous selection of frequency bands for a signature generation technique based primarily upon the speech content of a television audio signal. The bands **1** through **16** each have a bandwidth of 30 Hz. It is appreciated, however, that a different selection of bands and/or bandwidths may be adopted. In producing B_{adj} for each band B_n, it is preferable to employ values from nearby bands as this minimizes any distortions due to time delay differences at different frequencies. That is, signals of relatively close frequencies typically are delayed to a similar degree, although signals of substantially different frequencies can experience substantially different frequency delays.

The normalized band values produced by the normalization module **313** are then processed by a signature generation module **312**. Specifically, for each corresponding video frame interval, sixteen such normalized band values are supplied to the signature generation module **312**, one for each of the sixteen frequency bands. The signature generation module **312** utilizes a NOW-THEN processing technique to produce sixteen-bit audio signatures such that each signature bit is obtained based on a current value (or NOW value) of a corresponding frequency band and a previously obtained value (or THEN value) of the same frequency band produced from a frame preceding the current frame by a predetermined frame offset. More specifically, the received normalized frequency band values are written into a NOW-THEN circular buffer and the THEN values are obtained utilizing the predetermined frame offsets. The frame offsets may vary from band to band. However, in accordance with an advantageous embodiment, a frame offset of **8** is utilized for obtaining THEN values for each of the sixteen frequency bands. The signature generation module **312** produces a value DVAL for each frequency band in accordance with the following relation:

$$DVAL=(NOW-THEN)/(NOW+THEN)$$

The value of each of the 16 bits in the audio signature for the current frame and the bit values of corresponding mask word are determined in accordance with the value DVAL. That is, a signature bit is set to 0 if DVAL for the corresponding band is greater than 0, otherwise it is set to a value of 1. Similarly, each mask bit is set to a value of 0 if the absolute value of DVAL for the corresponding band is greater than a predetermined guard band value GRDVAL. For example, if DVAL has a range of 0–7FFF (Hex), a guard band value of 600 (Hex) may be employed, although different values of GRDVAL may yield acceptable results. The produced audio signature and its corresponding mask word for each frame interval are thereafter supplied from the audio digital signal processor **264** as hereinbefore described.

It is appreciated that the above technique for producing audio signatures which compares corresponding frequency band values displaced in time for each of a plurality of frequency bands can provide advantages over a technique which is based only on frequency or time displaced values, since the disclosed technique includes relatively more information in a given signature and provides a better balance of the types of information included in the signature.

EXPERT SYSTEM

The expert system is a software module which is stored within the control computer **30** and includes a number of "submodules" or programs identified as an occurrence filter, new segment detection and selective capture level submodules. Each of these sub-modules contained within the Expert System will now be described in detail.

Occurrence Filter

As previously mentioned, occurrence match data are supplied from each local site **16** to the central site **12** for compilation in the report **13** as illustrated by FIG. **1**. Thus, it is desired to reduce the amount of false match data supplied from the local site **16** to the central site **12** in order to improve the overall accuracy of the system **10** and to minimize the time spent by workstation operators at the central site **12**.

Basically, the occurrence filter sub-module receives match reports from the segment recognition subsystem **26** and assesses which, if any, of these received match reports is an erroneous or false match report. These detected false match reports are then excluded from a database of the control computer **30** to avoid transmission of false match reports to the central site **12**.

To assess whether a match report is erroneous, the occurrence filter examines each received match report from the segment recognition subsystem **26** in accordance with a plurality of predetermined rules. A preferred set of these predetermined rules will now be described with reference to the flowchart illustrated in FIG. **9**.

As shown in step **S10** of FIG. **9**, a determination is made as to whether the received match is definitely acceptable. A match is determined to be definitely acceptable if it satisfies at least one of two conditions, that is (1) a match is definitely acceptable if both the audio signature and the video signature for the respective segment have matched, or (2) if both the start and the end of the respective segment are temporally aligned with "strong cues". A cue, as employed in the occurrence filter, is a characteristic of the received signal other than the particular match being assessed by the occurrence filter. Examples of strong cues, as employed by the occurrence filter, are a fade-to-black (especially a fade-to-black of a video signal), as well as a match of a immediately preceding or succeeding signal segment. If the received match is found definitely acceptable in step **S10**, that is, the match satisfies one of the previously described conditions, the match result is stored within the database of the control computer **30**, as indicated in step **S20**.

If, on the other hand, the match is not found to be definitely acceptable, as indicated by a NO at step **S10**, then a determination is made as to whether the match is "definitely" unacceptable, as indicated at step **S30**. A match is determined to be definitely unacceptable if the match is not definitely acceptable (as determined in step **S10**), if it does not have a strong cue on either end of the corresponding segments, and if its corresponding segment substantially overlaps another segment having a match which is found definitely acceptable. If the match is determined as being definitely unacceptable, then the match is rejected as indicated in step **S40** and, as a result, information concerning the match is not stored within the database of the control computer **30**.

However, if the match is not definitely unacceptable, as indicated by a NO at step **S30**, a determination is made at step **S50** as to whether the respective segment has a strong

ADOBE – Exhibit 1002, page 198

JAFFE-ADOBE000232

cue on one end. If it is determined that the respective segment does have a strong cue on one end thereof, then the received match is subjected to confirmation matching as indicated by step **S60**, which is described in greater detail below. In this situation, a less stringent tolerance is utilized during the confirmation matching as compared to that employed in a step **S90**, as hereinafter described. That is the confirmation matching process of step **S60** will find a match between signatures having relatively higher match errors than in the case of step **S90** so that a match is more likely to be accepted in step **S60**. The result of the confirmation matching process will determine if the match is to be rejected or is to be accepted.

If, on the other hand, the respective segment does not have a strong cue on one end as indicated by a NO at step **S50**, then a determination is made, at step **S70**, whether the respective segment fits a profile of segments which typically false match. If the respective segment fits such a profile of segments which false match, then, as indicated at step **S80**, the match is rejected and information concerning the match is not stored within the database of the control computer **30**.

To determine whether a respective segment fits a profile of segments which false match, a false match rating R is determined for the respective segment. Such false match rating is determined by combining numerical ratings associated with respective ones of a plurality of characteristics in a linear fashion. These characteristics preferably include the following:

1. the length L of the respective segment: segments having a relatively short length are likely to false match;
2. the entropy of the key signature E: the entropy of a key signature is a measure of the dissimilarity between the matchwords within the key signature and is inversely related to the correlation therebetween. The key signature entropy is determined by a key signature generator, as hereinafter described and is thereafter supplied from the segment recognition subsystem **26** along with the corresponding match report. Key signatures having a relatively low entropy are more likely to false match than those having a relatively high entropy;
3. the correlator error threshold T: segments having a relatively high error threshold are likely to false match;
4. the distance D from missing the match: matches with actual correlator error counts which are close to the correlator error threshold are likely to be false matches; and
5. whether (M) the match being assessed was based on an audio or video signal: a match based on a video signal is more likely to false match than one audio based on an audio signal.

In accordance with one embodiment of a method for producing a false match rating, numerical values between zero and one are assigned to the characteristics L, E, T and D (the characteristic M not being utilized in this example) and a linear combination of the assigned values is formed to produce the false match rating R, as follows:

$$R=w_1L+w_2E+w_3T+w_4D$$

wherein w_1 through w_4 are respective numerical weights assigned to each of the characteristics for determining their relative importance in the determination of the false match rating R, and the values of the characteristics L, E, T and D have been converted to a normalized scale of zero to one. In the case of a television commercial recognition system, wherein higher values of R represent a relatively lower probability of a false match, exemplary values may be assigned to the characteristic L as illustrated in Table II below.

TABLE II

Length of Segment (in seconds)	L
10	0.0
15	0.30
20	0.40
30	0.80
45	0.95
60 or more	1.00

In this example, entropy E is measured on a scale of zero to 256, wherein **256** represents maximum entropy. Exemplary normalized values for E are illustrated in Table III below.

TABLE III

Entropy	E
130	0.0
135	0.10
140	0.20
145	0.50
150	0.70
160	0.80
170	1.00

Accordingly, the greater the entropy value, the higher the value assigned to E, reflecting the reduced likelihood of a false match for higher entropy values.

Further, in this example, the characteristic T representing the error threshold and ranging from 20 to 60 is assigned the values from zero to one in accordance with Table IV below.

TABLE IV

Error Threshold	T
20	1.0
30	0.90
40	0.70
50	0.40
55	0.25
60	0.0

As reflected by Table IV, higher values of the error threshold are assigned relatively lower values T, reflecting the relatively lower probability of a false match for higher error thresholds.

Exemplary values for the characteristic D representing the difference between the actual correlator error count and the error threshold are assigned values in accordance with Table V below.

TABLE V

Distance from Match Miss (in Error Count Units)	D
1	0.0
2	0.20
3	0.30
4	0.50
5	0.80
6	1.0

That is, the greater the difference between the actual correlator error count and the error threshold, the smaller is the probability of a false match.

ADOBE – Exhibit 1002, page 199

JAFFE-ADOBE000233

Finally, in this example, the weights w, through w_4 are assigned the values listed in Table VI below.

TABLE VI

Weight	Value
w_1	0.25
w_2	0.40
w_3	0.175
w_4	0.175

It will be seen that the sum of the weights is selected as 1.00. Therefore, since the values L, E, T and D have each been normalized so that each falls within a range of between zero and one, the false match rating R will likewise range from a low value of zero (representing a high probability of a false match) to a high value of one (representing a low probability of a false match).

In step S70, if the respective segment does not fit the profile of segments which false match, as indicated by a NO at step S70, then the corresponding match is subjected to confirmation matching as indicated in step S90. The tolerances utilized for the confirmation matching of step S90 are tighter than those utilized in step S60, as previously noted. Further, as in step S60, the results of the confirmation matching process in step S90 will determine whether the respective match is to be accepted and, thus, stored within the database of the control computer 30, or is to be rejected.

Another function of the occurrence filter is to determine whether the received match can be used as a cue for locating new segments or aligning other matches. Basically, the process used to decide whether a match is to be used as a cue is substantially the same as that described above in determining whether a match is acceptable. However, there are two exceptions. That is, (1) a match which appears to be unacceptable and is not near to any strong cues may be used as a cue, in case following matches can be aligned with it or else to find a new segment based upon a following match and, (2) segments which have a strong cue on one end but have a high false match rating, as described above, are not used as cues. However, in the case of exception (2), if confirmation matching later indicates an acceptable match, then the match may be reported to the database.

The storage buffer contained within the data capture subsystem 28, holds only a predetermined limited amount of data. Consequently, the occurrence filter preferably operates or reacts in a timely fashion so as to enable the audio and video data to be collected for a segment which requires such collection, for example, a new segment having a capture level 1 as hereinafter described.

In some instances, for example, when confirmation matching (which is relatively time consuming) is required, the information needed to decide whether a match is acceptable or unacceptable is often not available within the time constraint imposed on the occurrence filter. That is, all of the information needed to determine whether or not to accept a match may not be available at the time the match report is supplied to the control computer 30. To alleviate this problem, the occurrence filter makes a preliminary decision whether the match corresponding to the respective segment should be accepted at the time the match is reported. If a match is determined preliminarily to be acceptable (or is finally determined to be acceptable), it is reported to the database, whereas if the match is unacceptable, it is withheld from the database. The results the preliminary decisions are reviewed after a predetermined period of time, for example, approximately several minutes. During this predetermined time period, the confirmation matching processing is completed. Based upon the confirmation matching results, if a match which was previously not supplied to the database of the control computer 30 is now found to be acceptable, it will be supplied to the database as an acceptable match. On the other hand, if a match which was previously found to be acceptable and, as such, was reported to the database is now determined to be unacceptable, a match rescind signal is produced to delete the corresponding match. In general, matches which are initially determined as being definitely acceptable or unacceptable are not reviewed at the predetermined later time since their determination is not in doubt. However, where a matching audio or video signature is found to be definitely unacceptable before a match is found for the other corresponding video or audio signature, the match of the first signature will nevertheless be accepted since both of the corresponding video and audio signatures have matched.

Thus, with reference again to FIG. 3, the occurrence filter of the expert system 414 receives match reports from the segment recognition subsystem 26 and determines if such reports are false match reports. In certain situations, as discussed above, confirmation matching may be requested, whereupon the confirmation matching module 422, utilizing the segment recognition subsystem 26 as well as key signatures from the database 412 determines whether or not the match is acceptable. The results from the confirmation matching are supplied within a predetermined time period, to the occurrence filter. The occurrence filter supplies matches which are determined to be acceptable to the database 412. If the occurrence filter had previously supplied a match to the database which is later found to be unacceptable, the occurrence filter supplies a match rescind signal to the database control 416 to delete the respective match therefrom.

Confirmation Matching

The confirmation matching module is located within the control computer 30 (FIG. 2) and is utilized to evaluate matches of questionable acceptability at the request of the occurrence filter under the conditions described above. As an example, in certain situations, the audio or video sub-signatures but not both, may match. In this example, the occurrence filter may request confirmation matching to decide if the sub-signature which did not match initially in the recognition controller would nevertheless be regarded as matching a given key signature when compared thereto under standards which are more tolerant of match errors.

The confirmation matching module carries out a matching process which is similar to that utilized by the correlator 420 (FIG. 3) in the segment recognition subsystem 26. However, unlike in the correlator which is attempting to match keywords against a continuous stream of video and audio signatures, the confirmation matching module is attempting to match only one short length of a broadcast segment against one key signature. As a result, false matching is less likely to occur with confirmation matching than with the matching process performed by the correlator. Accordingly, error tolerances for the confirmation matching process can be considerably lessened or relaxed as compared to those employed in the correlator matching process, without resulting in an unacceptable false matching rate. This relaxation of error tolerances enables the confirmation matching module to determine whether a signature or sub-signature should have matched even though the correlator was unable to so determine.

Referring again to FIG. 3, a confirmation match request may be supplied from the occurrence filter module of the expert system 414 to the confirmation matching module 422. Such request may include the segment identification number, start and end times of the segment, the broadcast channel and a desired confirmation match tolerance. Upon receipt of such a match request signal, the confirmation matching module requests the segment signature data for the requested times from the segment recognition subsystem 26 and the relevant key signature from the database 412. After receipt of the requested information, the confirmation matching module 422 then compares the single key signature to the requested portion or segment of the broadcast signal in accordance with the desired confirmation match tolerance and, upon completion of the comparison, supplies the result (i.e. a match or no match) to the occurrence filter module.

The confirmation matching module performs the comparison by effectively moving the key signature along the segment signature as shown in FIG. 10. Essentially, the key signature is aligned with the segment signature at an initial position within an expected match zone and a match is attempted according to the match confirmation process described below. Each of a multiple of confirmation matches are also attempted by aligning the key signature at corresponding positions offset from the original position, respectively, by ±1, 2, 3, . . . , N frames. That is, in FIG. 10, N represents the number of frames which are to be checked on either side of the location within the expected zone of match, m(0) represents the respective keyword (which in confirmation matching is treated simply as another matchword), and m(x) represents the xth matchword in which $1 \leqq x \leqq 8$. Generally, the confirmation matching module computes a minimum total error count among all of the 2N+1 matching attempts which it compares to the sum of the error thresholds permanently assigned to the key signature and a confirmation match tolerance to make a decision whether a match exists.

More specifically, while the algorithm utilized by the confirmation matching module corresponds with that utilized by the correlator 420 in most respects, certain differences exist. These differences will now be described with reference to FIG. 10.

For each attempted confirmation match, a respective partial error count p is produced for each key signature match word, by comparing the matchword to the corresponding frame signature from the segment signature. A total error count is then determined by summing the number R (which has an exemplary value of 8) of the lowest partial error counts for each attempted match. In the preferred embodiment, since the keyword is considered simply as another matchword, the respective key signature contains nine matchwords. Thus, in calculating the total error count for each attempted match, the partial error count having the highest (or worst) error count is not utilized. The total error count for each attempted match is calculated for the N frames both before and after the location of the original location as shown in FIG. 7. The value of N should be carefully selected, since if N is too high false matching may result and, on the other hand, a value of N which is too small may not detect acceptable matches. In the preferred embodiment, N has a value of 60. The total error count having the lowest value is selected as the final error count. The final error count is then adjusted to account for any discarded partial error counts. In an advantageous embodiment, this adjustment is performed by using the following relation:

Adjusted Final Error Count=(Final Error Count)(8/R)

The confirmation matching module increases the error count or error threshold associated with the key signature by the error count specified by the confirmation match tolerance to obtain an error threshold value. The confirmation matching module then compares the final adjusted error count with the error threshold value. If the final adjusted error count is less than or equal to the error threshold value, a match is found to exist, whereupon a signal so indicating is forwarded from the confirmation matching module to the occurrence filter module. If, on the other hand, the final adjusted error count is greater than the error threshold value, then a match is not found to exist, whereupon a signal so indicating is supplied to the occurrence filter module.

New Segment Detection

The decision whether a new segment of interest (for example, a commercial) has been received is used to determine the information provided to the workstation operators for identification of such new segments. Referring again to FIG. 1, if the local site 16 identifies segments as complete new segments of interest, when in fact they are not (in which case they are referred to as "chaff"), workstation operator time is wasted in attempting to identify these segments. If the local site 16 does not correctly delineate the segment, so that, for example, only a portion of the audio and video information for the new segment of interest is provided to the operator, the operator's time may also be wasted and system accuracy is reduced.

Detection of new segments is carried out by the expert system and is primarily based upon several explicit and implicit cues. Explicit cues are normally received from the segment recognition subsystem 26 and may, for example, include video fade-to-black, sub-match reports, audio mute and scene changes. On the other hand, an example of an implicit cue is the segment duration. Each of these cues will now be described in more detail followed by a discussion of the operation of the new segment detection module.

Typically, commercials are broadcast with at least one video field having a substantially black level on each end. Since a commercial might have only one field of black on each end of the commercial, a fade-to-black on any field of the video signal is reported by the respective channel board to the new segment detection module through the segment recognition controller. Thus, a commercial boundary may be indicated by a fade-to-black, in which the boundary is normally at the start or the end of such fade-to-black. However, in some instances, the actual commercial boundary may be located in the middle of a fade-to-black. This may occur if nearly black scenes are detected as being black or if during an actual fade-to-black, the video signal begins fading up to the next commercial prior to allowing the fade-to-black to be completed. Although such fades-to-black do occasionally occur which do not correspond with commercial boundaries and which may be detected by the new segment detection module, the number of such spurious fades-to-black is relatively low as compared with the number of such audio mutes or scene changes, which are hereinafter described.

A match which has been accepted by the occurrence filter of the expert system is utilized as cue. As previously mentioned, although the segment recognition subsystem 26 may produce false match reports, the occurrence filter serves to identify and eliminate a substantial number of false match reports. As a result, a match which is determined to be acceptable by the occurrence filter is a reliable cue. Such a

match is also considered a relatively very strong cue either alone or especially in combination with a fade-to-black on either or both ends of a segment under consideration. For example, since commercials are typically broadcast in groups, or pods, such that the end of one commercial corresponds with the start of a subsequent commercial, determination of an acceptable match is a strong indication that a commercial is to follow. A match which is determined to be acceptable is also an important cue for informing the expert system where not to find a new segment of interest. As an example, the new segment detection module will not look for new segments in segments which have already had an acceptable match. That is, unlike a new segment, a segment which has already had an acceptable match associated therewith by the expert system, does not need to be forwarded to one of the workstations 14 for classification by an operator as previously described (since such classification has obviously already been performed for a match to have been detected).

Although the end of an acceptable match normally represents either the start of a subsequent segment or the start of a fade-to-black representing the true boundary, the match cue may not be precisely known in time. Since matches can occur on several consecutive frames, each match (audio and video) has a peak width associated therewith which is proportional to the uncertainty in time for the respective match. To compensate for such uncertainty, the new segment detection module attempts to align the respective match using other strong cues, such as another acceptable match or a fade-to-black, whenever possible.

Matches based upon temporary identification numbers (ID's) may represent segments which may differ from segments represented by matches which are based on permanent ID's. That is, matches based on temporary ID's (which have not been classified by a workstation operator) may represent only a portion of a segment, whereas matches based on permanent ID's have been viewed and judged correct by an operator at one of the workstations 14. The new segment detection module of the expert system preferably differentiates between matches obtained with signatures having the different types of ID's to apply greater weight to matches obtained with permanent ID signatures.

An audio mute representing a reduction of the audio signal substantially to a level representing silence, typically occurs at commercial boundaries. However, since audio mutes are very common throughout a commercial as well as in non-commercial segments such as normal programming, a large number of audio mutes do not indicate a commercial boundary. Accordingly, to rely on audio mutes to detect both ends of a segment can lead to the selection of significant amounts of normal programming as segments of interest, or else incorrectly dividing one commercial into two partial segments, neither of which will correctly match in the future since its length is incorrectly recorded. Thus, an audio mute is considered a relatively weaker cue than the previously described fade-to-black or an acceptable match cue. As a result, the use of an audio mute as cue needs to be restricted or else excessive chaff will be generated. Further, when an audio mute does indicate a commercial boundary, the boundary may not lie exactly at the start or end of the audio mute, but instead may lie at some undefined location within the audio mute. As a result, long audio mutes are typically unusable as cues due to the uncertainty of the exact location of the commercial start or end.

A scene change is a abrupt change in the video picture which occurs between frames. Since scene changes within segments are common, in addition to those occurring at the commercial boundaries, a scene change is considered a relatively weak cue. Nevertheless, scene changes may be very helpful. For example, many commercials which do not have a fade-to-black at a boundary do have a scene change at that point. Although the scene change by itself is a weak cue as previously mentioned, the scene change can be combined with an audio mute to form a stronger cue. For example, the scene change may be utilized to locate the commercial boundary within an audio mute.

Implicit Cues

One of the more important implicit cues is segment duration. Typically, commercials are broadcast in standard or nominal lengths, for example, lengths of 10, 15, 20, 30, 45, 60, 90, or 120 seconds. Some of these commercial lengths occur more frequently than others. In particular, 30 second commercials are believed to occur most frequently. It is believed that the frequency of occurrence of the various commercial lengths is represented as follows, wherein the frequency of occurrence of a commercial of duration t (in seconds) is represented as CL_t:

$$CL_{30} \gg CL_{15} \gg CL_{10} > CL_{60} > \{CL_{20}, CL_{120}, CL_{90}, CL_{45}\}$$

That is, as an example, commercials having a length of 10 seconds are believed to occur more frequently than commercials having a length of 60 seconds. The intervals of the more frequently occurring lengths are considered to provide stronger cues than those associated with the less frequently occurring lengths.

The deviation from the nominal segment length is also part of the segment duration cue. More specifically, commercials or segments of interest rarely conform with the nominal lengths of such segments (for example, 30 secs., 15 secs., etc.). Instead, they are normally slightly shorter or longer than the corresponding nominal length. Typically, a segment is shorter rather than longer than the corresponding nominal length. That is, since each commercial or segment of interest is produced to fit within a predetermined block of time, it is considerably less cumbersome to have the segment of interest slightly smaller than the nominal length whereupon frames (such as fades-to-black) may be added, instead of editing the segment of interest to fit within the predetermined block length. Segments which are longer than the corresponding nominal length are normally the result of errors occurring either at the broadcast station or at the receiving station. For example, it is believed that a most likely length deviation for a new segment of interest is between approximately 0.0 to −0.2 seconds with a peak located at approximately −0.13 seconds. Typically, for a respective segment, the further the length of the segment deviates from the peak nominal length, the less likely the segment is a segment of interest. As is appreciated, the likelihood that a segment is a segment of interest decreases rapidly as the segment length increases over the nominal length.

Since, as previously mentioned, commercials or segments of interest are typically broadcast in groups or pods, when one new segment is detected, this indicates that other new segments may be adjacent thereto. Therefore, a detected new segment is a cue for detecting other new segments. However, the strength of the new segment as a cue depends on the likelihood that the new segment is a new segment of interest which, in turn, depends on the cues upon which the new segment is based.

It is assumed that the probability of detecting a new segment having a predetermined length, with certain cues,

which does not correspond to a segment of interest (or in other words a chaff segment) is relatively independent of the length selected. As previously mentioned, interpreting chaff segments as new segments of interest increases the processing time of the system **10** (FIG. **1**) and thereby increases the overall operating cost of the system. Thus, it is desirable to select segments as possible new segments of interest having time intervals or segment lengths which are likely to correspond to new segments of interest.

It is considered, therefore, to be more productive to spend operator time searching for segments having a length of 30 seconds which, as previously mentioned, are believed to be common, than it is to spend operator time looking for segments having a length of 45 seconds which are not believed to occur as frequently. While this allocation of operator time means that a 45 second new segment is less likely to be detected than a 30 second new segment, the result is a relatively high overall system accuracy with minimization of operating costs.

FIG. **11** illustrates the signal flow in carrying out the detection process. A desired broadcast signal in a given channel is received by a respective one of the converters **24** and converted into baseband video and audio signals which are supplied to the channel board **402**. The channel board **402** supplies cues pertaining to the new segment of interest to the segment recognition controller **404** which also receives match information from the correlator **420**. The cues along with match reports are supplied from the segment recognition controller **404** to the expert system **414**. The expert system **414** examines the received information to determine if possible new segments indicated by the cues are new segments of interest. If any of the indicated segments is found to be a new segment of interest, the expert system **414** supplies a signal to the segment recognition controller **404** requesting the respective segment signature which is then collected and supplied to the expert system. Upon receipt by the expert system, such new segment signature is supplied through the database control **416** to the database **412**. Further associated signals supplied by the expert system to the database **412** include the time of occurrence, the channel, the segment identification number, the key signature and the audio and video threshold values. Further, in certain situations, as previously described, the expert system **414** may supply an initial A/V capture or threshold value signal to the database control **416** prior to determining a final threshold value. If, in these situations, it is later determined that the initial threshold value was incorrect, the expert system **414** will supply a threshold value change or rescind signal to the database control **416** to correct the entry in the database **412**.

The operation of the new segment detection module will now be discussed.

In accordance with one operational node, the new segment detection module scans the cues in a received signal to detect a segment having a standard length for a segment of interest. The first segment detected which has such an interval and satisfies predetermined criteria described hereinbelow is accepted as a new segment of interest. Since the first interval which satisfies such requirements is accepted, subsequent new segments which may conflict therewith (i.e., another segment occurring during the same period of time) are not considered. Therefore, the segment which is detected and accepted is dependent upon the order in which the cues are scanned as hereinafter described.

The cues are stored in a cue deque in which a node is established each time there is an on-off transition of any of the cues. These nodes are sorted by time. Matches are supplied to the deque by the occurrence filter when they are determined to be acceptable for use as cues. These cues are then scanned by either specifying a start location in the deque or by specifying a desired time. If a time is provided, the latest point in the deque which occurred after a predetermined fixed time delay (e.g., approximately 80 seconds) is used as the initial scanning time to compensate for the delay in reporting matches as compared to cue reports.

The cues may be scanned by more than one pass and, in a preferred embodiment, two passes are utilized. The first pass scans for all cues except audio mutes, and the second pass scans the cues for audio mute based segments. This scanning process will now be more fully described.

The cues are scanned backward in time utilizing two nested loops. In an outer loop, the deque is scanned backward for appropriate cues for the tail (or end) of a segment and in an inner loop the deque is scanned backwards from the current tail position in search of appropriate cues for the head of a new segment. In this manner, all possible new segments which contain a plausible cue on each end are detected. Each of the time intervals is evaluated to determine if, given the respective length and the associated cue types, it represents an acceptable new segment of interest. That is, the new segment detection module determines, for a respective segment, whether the cue types are acceptable and then determines if the length of the segment in combination with these cues indicates an acceptable new segment of interest.

If an interval is indicated to be a new segment of interest, it is assigned a segment identification number and is stored in the cue deque as an occurrence. Afterwards, a selective capture level module is utilized to determine an appropriate audio/video capture level value, as hereinafter described. Further, the segment signature is obtained from the segment recognition subsystem **26** and the respective signature is then supplied to the database **412** of the control computer **30**.

FIG. **12** illustrates the above-described steps performed by the new segment detection module. As shown therein, processing begins at step **S100** wherein a desired portion of the received broadcast is examined to locate all intervals between cues. Afterwards, as shown in step **S110**, each of the intervals located in step **S100** is examined so as to determine if the respective start and end cues are plausible. Thereafter, as shown in step **S120**, the acceptability of each interval which has plausible cues on its respective ends is determined based upon the respective nominal length of the interval, the deviation from this nominal length and the combination of the start and end cues. If the interval is determined to be acceptable, then as indicated in step **S130**, the audio/video capture level is determined by the selective capture level module. Thereafter, the newly accepted segment of interest is supplied to the database **412** of the control computer **30** as shown in step **S140**. If, on the other hand, in step **S120**, the respective interval or segment is rejected, then further processing for this segment is not performed.

After locating a new segment, the outer loop is reset so as to continue from the start of the newly detected segment. The outer loop terminates upon encountering a cue Which has already been checked as a possible tail cue. This can be determined by examining cue examined flags. That is, each node in the deque which has already been checked as a possible tail cue has a cue examined flag set. Since, in the preferred embodiment, there are two scanning passes, there are two cue examined flags. On the other hand, the inner loop terminates when it locates a cue separated in time from the current tail cue by an amount longer than that of any standard segment (e.g., 120 seconds).

Two passes are utilized so that the audio mute based segments may be given a lower priority than other segments.

More specifically, in a preferred embodiment, the second pass is at a scan point 30 seconds later than in the first pass. This enables the first pass to locate all segments up to 30 seconds in length which are not based on audio mute cues before checking for audio mute based segments in the second pass. As a result, the lower probability (or less likely to be acceptable) audio mute based segments will not be detected prior to detection of segments of interest having a higher probability of occurrence, for example, those based upon matches and fades-to-black having lengths up to 30 seconds. As previously mentioned, the first detected segment may be utilized without considering any possible conflicting segments (although it is preferable to resolve such conflicts, as described hereinbelow). In such a situation, it is desirable to utilize the two passes as hereinbefore described. Further, since all audio mute based segments are given a capture level 2 by the selective capture level module as hereinafter described, so that the respective audio and video data are not collected when such segments have not been encountered previously, the delay in scanning can be set to an even longer value. This would further minimize blocking of a higher probability based segment by an audio mute based segment.

Determining whether a cue is appropriate for the start or end of a segment involves careful consideration. For example, in the case of an occurrence cue, it may be necessary to ensure that a start occurrence cue which may be useful as a tail cue is not, at the same time, the end of another occurrence. This can be determined by checking that start and end occurrence flags are not both set. As another example, it may be necessary to determine if a fade-to-black is associated with an occurrence, whereupon this occurrence can be used to increase the cue strength. That is, if the start of a fade-to-black is under consideration as a possible segment tail cue, then the end of the fade-to-black should be examined to determine if it is the start of an associated occurrence. If this is so, the strength of the cue can be increased.

The characteristics utilized in the new segment detection module described above to determine the acceptability of a segment as a new segment of interest will now be more fully described.

The maximum allowable deviation from the nominal length is determined. However, in such determination, the more frequently occurring nominal lengths are favored, by providing them with relatively large deviation tolerances, to increase the chances of detecting a new segment of interest. Separate tolerances are preferably utilized for deviations smaller and larger than the nominal length, in which the tolerance for the deviation shorter than a nominal length is typically larger than that for the deviation larger than the nominal length.

The cues for each interval are used to adjust the maximum allowable deviation from the nominal length for the segment under consideration. This is done by analyzing the cues on the ends of the respective segment to determine which of the cues on each end is the strongest. Occurrence cues are considered to be the strongest, followed in turn by fades-to-black and audio mutes. That is, the tolerance is adjusted according to the strength of the cues on both ends of the segment.

Uncritical use of audio mutes as cues can generate a relatively large number of chaff segments. However, audio mute based segments may be acceptable with an audio mute as a cue on one end provided a relatively strong cue is present on the other end. Further, since audio mutes having a relatively short length occur frequently and audio mutes having a relatively long length normally do not allow accurate determination of segment ends, only audio mutes having a length which lies within a predetermined range are utilized. Nevertheless, all such audio mute based segments are given a capture level of 2by the selective capture module. To further limit the number of chaff segments detected, only segments having a more frequently occurring nominal length are permitted to be based upon audio mutes as cues. Furthermore, while segments with a match on one end and an audio mute on the other will normally be acceptable, segments having a newly detected segment on one end and a match on the other are not acceptable because the newly detected segment may be based upon an audio mute cue. In this situation, a plurality of segments may be detected as new segments which are based on audio mute cues on both ends. Therefore, segments based on occurrence cues on one end without an associated additional strong cue, for example, a fade-to-black cue, and an audio mute cue on the other end may not be utilized.

The audio mute may be utilized in the splitting of segments. Since commercials having a length of 30 seconds occur most frequently, in a television commercial recognition system, segments having lengths equal to multiples thereof, for example, 60, 90 or 120 seconds, may be split into a plurality of segments each having a length of 30 seconds. These segments may be split by utilizing the audio mute in addition to a scene change as split cues. That is, the segment is examined at each 30 second interval to determine if an audio mute and a scene change are present, whereupon the segment is divided. The splitting of segments in this fashion is different from that performed on long segments, wherein new segments having a length over a predetermined value, for example, 60 seconds are split in two at an arbitrary location even if the above-mentioned audio mute and scene change split cues are not present.

When relatively high numbers of fades-to-black occur, or when a fade-to-black is detected for a relatively long period of time, this normally indicates that a signal having a relatively poor quality is being detected.

Excessive fades-to-black may be the result of a poor signal or noise at the input. Attempting to detect new segments from such a poor quality signal usually results in detecting chaff segments. To correct such a situation, cues are not accepted from a portion of a signal which is determined to have such a relatively high occurrence of fades-to-black. Cues which are thus not accepted may not be used for a new segment start or end cue.

The above described cue rejection is performed by utilizing several factors, for example, the amount of fade-to-black time, the number of fade-to-black on/off transitions as hereinafter described, and the amount of non-fade-to-black time occurring during the previously described inner loop. Variables corresponding to each of these factors are initialized upon detecting a suitable tail cue (before starting the inner loop scanning). Thereafter, as the inner loop is scanning for a head cue, the signal is monitored to detect the above factors. If a possible new segment is detected, the respective segment is examined for the presence of the above factors. If the number of occurrences of these factors in a segment exceeds a predetermined maximum value (for example, a predetermined maximum amount of fade-to-black time and/or a maximum predetermined number of fade-to-black on/off transitions), then the segment is not accepted as a new segment.

In accordance with a second operational mode, the new segment detection module carries out the process illustrated in FIG. 13 for detecting new segments of interest. In a first step S400, the new segment detection module scans the cues

and picks out all intervals that are reasonable possibilities for new segments and places such intervals in a list of possible segments for later re-examination. Subsequently, processing is delayed in a step **S410** for a predetermined interval selected to maximize the possibility that segments which may overlap the already listed possible segments will be detected before it is determined which of the conflicting segments shall be accepted and which discarded. The delay interval may, for example, be at least 35 seconds so that no 30 second segments (which occur most frequently) are lost due to insufficient information on potentially overlapping segments.

After the decision delay, processing continues in a step **S420** in which each possible segment is compared with all other segments in the list to determine if conflicts are present. If so, a heuristic is applied to decide which segment shall be accorded a higher priority based upon a linear combination of relevant factors. Such factors include nominal length, associated cues, and deviation from nominal length. Once the conflicting segments have been thus prioritized, the higher priority segment is reported to the database (with possible audio/video collection for viewing at a work station of the central cite) and the lower priority segment is marked as a discarded segment. However, after a further delay, represented by a step **S430**, the discarded segments are reexamined to determine if a conflict still exists with an accepted segment. If not, the previously discarded but nonconflicting segment is reported to the database as a threshold **2** segment (as explained hereinbelow).

The manner in which the conflict assessment in the prioritizing process of step **S420** can result in the later acceptance of a previously discarded segment is illustrated by the following example. In one possible scenario, a segment A is assumed to overlap and occur later than a segment B, while the segment B overlaps and is assumed to occur later than a segment C. It is assumed further that segments A and C do not overlap. If segment B is first compared to segment A, such that segment B is given priority over A, then segment A will be rejected. However, segment B will be compared to segment C, and if segment C is preferred then segment B will also be rejected. Once segment B has been rejected, segment A is no longer conflicting, and it can, therefore, be accepted even after a prior rejection.

In accordance with a third mode of operation of the new segment detection module, as illustrated in FIG. **14**, in a step **S500** the cues are scanned to locate possible segments which would be acceptable as new segments of interest according to the criteria described hereinabove. In a following step **S510**, processing is delayed, for example, for as long as five minutes to ensure that all related possible segments have also been detected. Thereafter, in a step **S520** attached, overlapping and conflicting segments are placed in respective groups of related segments for further processing, for example, by marking a node established for each such segment in an appropriate deque with an arbitrary number identifying its respective group.

Thereafter, a two step heuristic is carried sequentially in steps **S530** and **S540**. In step **S530**, the new segment detection module determines the acceptable splits among the various segments under consideration. A split is a possible subdivision or grouping of the identified segments based upon accepted nominal lengths for segments of interest. For example, with reference to FIG. **15**, a split tree for a 120 second segment with a fade-to-black at each 30 second boundary therein is illustrated. In FIG. **15**, the possibilities for splitting the 120 second segment are arranged in a tree structure where each path from the root **600** to a leaf node (for example, leaf nodes **602** and **604**) represents a respective way to split the 120 second segment. The numbers 30, 60, 90 and 120 represent the duration in seconds, or segment length, of a possible segment formed from the main 120 second segment. It is seen that a segment can appear more than once on the diagram.

Once the possible ways of splitting the given segment have been defined in accordance with the split tree, the tree is traversed and each path (that is, possible combinations of segments) is evaluated in accordance with a set of predetermined rules for determining acceptable splits.

The predetermined rules which are employed in evaluating the acceptability of the possible splits are based on the nominal length of the main segment and the possible subsegments, as well as audio/video (A/V) thresholds determined therefor as explained hereinbelow in connection with selective capture level determination. Essentially, the rules are designed to avoid A/V threshold splits, that is, a division of a segment of interest into sub-segments having different A/V thresholds. The rules are designed also to favor splits into frequently encountered lengths such as 30 second segments. For example, an A/V threshold **2** segment is split into a plurality of sub-segments if all sub-segments have an A/V threshold of **1**. In addition, a 45 second segment will be split into segments encountered with greater frequency, such as a 15 second segment and a 30 second segment. The various rules themselves are stored in a table permitting future modifications.

If the application of the foregoing rules results in several acceptable splits, the still conflicted splits are prioritized in accordance with the following additional rules. First, splits which yield the greatest duration of A/V threshold **1** segments are favored over others. If there is then more than one split remaining, the splits are rated on a point scale based on the nominal lengths of each segment in the split, such that commonly occurring segment lengths are favored. That is, a points-per-second value is assigned for each nominal length and then multiplied by the length of the segment to accumulate a total points score for each nominal length. For example, if 30 second segments are accorded 3 points per second, while 15 second and 45 second segments are each accorded 2 and 1 point per second, respectively, the 45 second segment would yield a point total of 45, whereas the 30/15 split would yield a point total of 120, which thus favors the split. Accordingly the scale is constructed to favor those splits yielding segments of more commonly occurring lengths. If after application of the foregoing rules, more than one split remains, one is then chosen arbitrarily.

Once the split analysis has been carried out in step **S530**, conflict analysis is carried out in step **S540** according to which the most likely segment among a plurality of segments overlapping in time (which are, mutually exclusive) is given priority. Segments which are part of a split are now considered individually. Each pair of conflicting segments are rated in accordance with a heuristic explained below and the best is chosen. By pairwise comparison, a single most preferred segment is chosen. If after this choice is made, there are less preferred segments which do not conflict with this choice, they are also accepted.

The heuristic is a rating system which generates a linear function of the properties for each segment, namely, nominal length, cues and deviation from nominal length. A score for each value of a given property is assigned based on the following principles. Occurrence cues are considered much stronger than new segment cues which are in turn considered

ADOBE – Exhibit 1002, page 205

JAFFE-ADOBE000239

to be stronger than a single fade-to-black. With respect to deviation from nominal length, segments are more likely to be shorter than nominal length than longer, and the more their length deviates from the nominal length, the less probable it is that a segment of interest has been detected. The most probable deviation is between 0–0.2 seconds. In the case of nominal length, as noted above, 30 second segments are the most frequently encountered, followed by 15 second, 10 second and 60 second segments, in that order, while 20, 45, 90 and 120 second segments are considered to be quite rare. Overall, the cues are weighted more heavily than the other two properties. Where, however, the frequency of nominal length property is the only consideration, a special case arises. Namely, if both of the segments under consideration have an A/V threshold of **1** and one segment is contained in the other, generally the longer segment will be preferred and an appropriate point value would then be assigned depending upon the nominal lengths of the two segments.

Selective Capture Level

The selective capture level module serves to reduce processing of chaff segments at the local sites **16** to avoid reporting these to the central site **12** which would waste workstation operator time. A chaff segment is a segment which has been found by the expert system to be a new segment of interest, when in fact it is not. For example, a chaff segment may be a news brief or a portion of normal programming bounded by cues and having the same length as a segment of interest.

Processing of chaff segments increases the processing time of the system **10** (FIG. 1) and its operating costs. That is, a segment that is found to be a new segment of interest, but which is actually a chaff segment, is transmitted from the local site **16** through the central site **12** to one of the workstations **14** for processing by an operator, so that a high chaff rate substantially increases the time that the operators must spend in trying to classify new segments. Thus, treating chaff segments as new segments of interest disadvantageously increases the communication between the local sites **16** and the central site **12**, increases the operator workload at the workstations **14** and increases the processing which must be performed at the local site **16**.

The selective capture level module divides segments found to be potential new segments of interest into two groups, namely, segments which are more likely to be segments of interest (non-chaff) and segments which are less likely to be segments of interest. The segments which are more likely to be segments of interest are assigned an audio/video (A/V) capture level **1**, whereas the segments which are less likely to be segments of interest are assigned an audio/video (A/V) capture level **2**. Upon detecting a possible new segment of interest, whether assigned an A/V capture level of **1** or **2**, a key signature is produced therefor and stored, as explained hereinafter. The audio and video (A/V) data for a segment having an (A/V) capture level **1** are immediately collected for transmission to the central site upon detection of the new segment of interest. On the other hand, the A/V data for a segment having an A/V capture level **2** are collected only after its previously stored key signature has had at least one match. That is, a segment assigned an A/V capture level **2** will be broadcast and detected at least twice (once to detect the segment as a new segment and once again due to a match on its key signature) before the A/V data associated therewith are collected. If its key signature does not produce a match within a predetermined time period, it is purged from the system.

Only segments which have their A/V data collected are supplied from the respective local site **16** through the central site **12** to one of the workstations **14** (FIG. 1). Most segments of interest are broadcast more than once, while chaff segments are seen only once. Accordingly, by assigning an A/V capture level of **2** to segments which are less likely to be segments of interest, so that their A/V data are not collected until a subsequent match on such segments' key signatures, substantial operating cost savings can be achieved.

In accordance with a technique for assigning capture levels in a television commerical recognition system, a new segment is assigned a capture level **2** if it satisfies one of the following conditions:

1. If the sole cue at either end of the new segment is an audio mute cue. Since, as previously discussed, audio mutes occur frequently both at segment boundaries and within segments, new segments based on an audio mute cue are likely to be chaff segments.
2. If the new segment is not close or proximal to a group or pod of commercials. Since most commercials are broadcast in groups or pods, a new segment is likely to be close to such a pod. Proximity to a pod is advantageously assessed by determining the proximity in time of the new segment to another new segment or a segment having an accepted match. Since the proximity of a segment having an accepted match to the new segment being assessed provides a more reliable indication of pod proximity than the proximity of another new segment thereto, another new segment is considered proximal only if it comes within a proximity range which is narrower than a proximity range established for segments having accepted matches.
3. If the nominal length or duration of the new segment is an infrequently occurring commercial length, for example, nominal lengths of 20, 45, 90 or 120 seconds. Since commercials rarely have these lengths, a new segment having such a length is likely to be a chaff segment.
4. If the new segment deviates from the nominal length by an amount close to a predetermined length deviation limit adopted for determining the acceptability of the segment as a new segment of interest. For example, if the lower length deviation limit for a 30 second commercial is one second such that segments having durations less than 29 seconds are deemed not to be new segments of interest, a segment having a duration of approximately 29.1 seconds will be given on A/V capture level of **2**. The more a new segment deviates from nominal length, the more likely it is a chaff segment.

On the other hand, a potential new segment is assigned a capture level **1** if it is not assigned a capture level **2**.

It is appreciated that conditions 1, 3 and 4 are readily ascertained at the time a new segment of interest is found. However, ascertaining whether a new segment is proximal to a pod in accordance with condition 2 requires an assessment of subsequently received signals for matches and other new segments. Therefore, as an example, if the new segment being assessed is the first segment in a pod, it is not known immediately that the new segment is proximal to the pod. In accordance with an advantageous embodiment, new segments which satisfy all of the conditions for capture level 1 except condition 2 are initially accorded A/V capture level

1 so that the corresponding A/V data is stored in the database to permit later transmission to the control site. This determination is reviewed again after a predetermined time, for example, several minutes, at which time if the segment is still not found to be proximal to a pod, the A/V capture level of this segment is changed to capture level 2. This procedure enables the retention of the segment's A/V data pending a complete assessment of all information necessary to determine when condition 2 obtains. If this delayed assessment then established that the segment should be assigned A/V capture level 1, the A/V data thereof is still available for transmission to the central site. Otherwise, it is deleted from the database.

The use of the selective capture level technique described above allows the expert system to relax its criteria for determining which segments are likely to be segments of interest while maintaining an acceptable processing burden on the system **10** (FIG. **1**). Accordingly, the expert system is thereby able to employ new segment criteria which permit the acceptance of relatively more segments as new segments of interest, for example, by adopting relatively wider length tolerances. Accordingly, any new segments of interest which would only satisfy the relaxed criteria may be detected where they would otherwise be missed. As a result, the overall system matching accuracy can be increased.

FIG. **16** illustrates the signal flow for capturing audio and video data. As shown therein, baseband video and audio signals are supplied from the channel boards **402** of the segment recognition subsystem along cables **431** and **439**, respectively, to the data capture subsystem **28**. The data capture subsystem **28** includes a video capture board **432**, a compressed video ring buffer **430**, a data capture controller **434**, a compressed audio ring buffer **436** and an audio capture board **438**. The received baseband video signal from the cable **431** is supplied to the video capture board **432** which continuously provides newly received video signals in compressed form to the compressed video ring buffer **430** which maintains a current record of the most recently received compressed video signals, for example, those received during the last 3 to 7 minutes. Similarly, audio baseband signals from the cable **439** are supplied to the audio capture board **438** which continuously provides newly received audio signals in compressed form to the compressed audio ring buffer **436** which likewise maintains a current record thereof.

The data capture subsystem **28** communicates with the control computer **30** which, in turn, utilizes the expert system **414**, the data base control **416**, the data base **412**, an A/V collection control **440** and a disk **442**. As an example, if a new commercial has been detected which has a threshold or capture value of **1**, the expert system **414** supplies a signal so indicating to the database control **416**. Upon receipt of such a signal, the database control **416** supplies a command signal requesting that the respective audio and video data be transferred to the A/V collection control **440** which, in turn, supplies a corresponding request signal to the data capture controller **434**. Upon receipt of such a signal, the data capture controller **434** supplies respective control signals to the video ring buffer **430** and the audio ring buffer **436**, whereupon the requested video and audio signals are supplied to the data capture controller **434**. The requested audio and video signals are thereafter supplied from the data capture controller **434** to the A/V collection control **440** which, in turn, supplies the same to the disk **442** for storage. Further, the A/V collection control **440** supplies the identification number of the segment along with a signal indicating whether the audio and video data have been collected for the respective segment to the data base **412**. Further, in certain situations as previously described, the expert system **414** may supply a rescind signal to the database control **416**. Such signal is thereafter supplied to the A/V control **440** whereupon the appropriate A/V data file is deleted. In these situations, the A/V control **440** supplies a confirmation signal to the database control **416** which confirms the deletion of such files.

KEY SIGNATURE GENERATION

Upon detection of a new segment of interest, as noted above, the system **10** produces a key signature for the segment which is later used to recognize a rebroadcast of the same segment by comparing or matching the key word and eight match words of the key signature with corresponding frame signatures of a segment signature produced for the rebroadcast segment. With reference to FIG. **17**, the control computer **30** implements a key signature generator module **410** which receives sequential frame signatures for the segment of interest, referred to as a segment signature, to produce a key signature therefrom. This key signature is thereafter supplied to the segment recognition subsystem **26** for use in subsequent matching operations.

It is appreciated that a relatively large number of segments of interest (for example, commercials) will be received at each of the local sites **16** (FIG. **2**) and it is desirable that each such key signature have a relatively small size to minimize the amount of memory needed. It is further desirable that the key signatures readily match upon a rebroadcast of the respective segment, while avoiding false matching. Accordingly, the key signature generator module **410** produces key signatures which are advantageously small in size and which are selected and structured to maximize the likelihood for a match on a rebroadcast of the respective segment, while reducing the potential for false matching.

A segment signature for key signature generation is received for processing by the module **410** in the form of combined audio and video frame signatures. The module **410** then separates the received segment signature into audio and video segment signatures which it processes separately. For example, the key signature generation module may perform two separate processing cycles, that is, one for the video segment signature and one for the audio segment signature. As a result, typically at least one audio key signature (or sub-signature) and one video key signature (or sub-signature) is produced for each segment signature, each having the same data format.

Each key signature preferably includes 16 elements which will now be described in detail.

1. Segment identification number (Segment ID)—this identification number uniquely identifies the segment identified by the key signature and, for example, in a television commercial recognition system may be used to more readily associate commercials with their respective key signatures. As described hereinbelow, the module **410** under certain circumstances generates up to four video key signatures and four audio key signatures for a given segment. Accordingly, the segment ID is comprised of a number divisible by five together with a number from 1 to 4 indicating the number of video or audio key signatures produced for the segment.
2. Keyword—a 16-bit keyword is selected for each segment from among the frame signatures thereof comprising its segment signature. As described above, the keywords are used by the segment recognition subsystem **26** as an index to the key signature database to minimize the time required in detecting a match.

3. Keyword offset—this represents the distance from the beginning of the respective segment to the keyword. This offset may be expressed, for example, as the number of frames from the beginning of the segment or in terms of time from the beginning of such segment.

4. Matchwords—there are a plurality of 16-bit matchwords (e.g., 8) in each key signature. The matchwords of a given key signature are used by the segment recognition subsystem **26** during the matching operation after the associated keyword has matched an incoming frame. That is, as previously described, each received frame signature is compared with all stored keywords. Upon detection of a match between an incoming frame signature and a keyword (for example, based upon a coincidence of at least fifteen corresponding bit values of the frame signature and the key word), all of the matchwords associated with this keyword are then compared to the appropriate incoming frames as determined by the matchword offsets, described below. If the total number of unmasked bits which do not match in value combined with one half the number of bits of the compared frame signatures which are masked, does not exceed a predetermined error count or threshold (described below), then a match is found. Criteria for selecting the keyword and matchwords for the key signatures are described hereinafter.

5. Matchword offset—there is a matchword offset for each of the matchwords. Each matchword offset indicates the position of the respective matchword relative to its keyword. As with the above-described keyword offsets, the matchword offsets may be expressed in terms of time differences or numbers of frames. These matchword offsets are used to indicate which of the incoming frame signatures of the broadcast segment are to be used for comparison with the matchwords in the key signature when a keyword match has been detected.

6. Signature type—the signature type identifies whether the signature is an audio sub-signature or a video subsignature. Since the audio and video key sub-signatures have the same format, this element is used to distinguish them.

7. Error count—the error count or error threshold is generated by the key signature generation module for each key signature generated and indicates the maximum number of errors which may be allowed during the matching process before the match being considered is rejected as unacceptable. The error count may be based upon specific characteristics of the generated key signature, for example, the expected dependability of the corresponding segment and the likelihood of the key signature false matching. An advantageous technique for determining the error count utilizes the probable number of bit matches for the matchwords, as described below, rounding this number down and subtracting the resulting number from the total number of possible matches. The resulting error count is made lower in the case of shorter segments which are more likely to false match. It is appreciated that, under certain conditions (e.g., due to noise), the key signature may not match perfectly to a rebroadcast of the corresponding segment. The error count compensates for such anticipated discrepancies to enable detection of the rebroadcasted segment.

8. Frame count—the frame count indicates the number of frames contained with the key signature which, in the preferred embodiment, has a value of 8.

9. Length—this refers to the number of frames in the respective segment.

10. Match rules—match rules are generated by the key signature generator module for each segment represented by one or more key signatures in the database and are guidelines utilized by the expert subsystem **414** in determining whether or not to accept a match of the key signatures for such segment. If there is a relatively high probability that both the audio and video sub-signatures will false match, the match rules require both the audio and the video key sub-signatures to match in order for a match to be accepted. If, on the other hand, it is determined that neither the audio nor the video key sub-signatures are likely to false match and, in fact, may have difficulty in matching, the match rules accept a match if either the audio or the video key sub-signatures match.

The match rules are based on the probability that the sub-signatures will correctly match a rebroadcast of the corresponding segment, as well as the probabilities that the subsignatures will false match. The manner in which the probability of a correct match is assessed is discussed hereinbelow. The probability of false matching or false match quotient is determined as the average of a first value inversely proportional to the amount of information in the signature (that is, the greater the number of bits which are the same, the higher the first value becomes) and a second value which is a normalized clumping value for the signature. The normalized clumping value is obtained by multiplying the number of key signatures in the database having the same keyword as the signature under consideration, by the a priori probability that a frame signature (or any single bit permutation thereof) corresponding with that keyword will be produced. The normalized clumping value represents the tendency of key signatures to be concentrated (or clumped) under a given keyword.

11. Number of mask bits set—this number represents the sum total of all of the mask bits which are set for the keyword and all of the associated matchwords.

12. False match quotient—this represents the likelihood of the respective key signature providing a false match when compared against a segment signature and is determined in the manner discussed above in connection with the match rules.

13. Sharpness—there are often multiple consecutive frames in a segment which are substantially identical, for example, video signal frames corresponding to a single scene. Such groups of substantially identical consecutive frames are called runs. Sharpness represents the rate of change in the bits of the frame signatures at the ends of the runs from which the key signature was derived and is used to delineate the edges of the runs.

14. Match probability of the other corresponding key subsignature—as previously mentioned, the key signature may be divided into two sub-signatures, that is, one for audio and one for video. The match probability referred to herein is the probability that the other corresponding sub-signature will match for the respective segment. For example, consider the situation in which the segment recognition subsystem **26** detects an audio match, but not a video match, for a particular segment. This matching information is thereafter supplied to the expert system whereupon, if the audio key sub-signature has indicated therein that there is a relatively high match probability for the other sub-signature (i.e., the video sub-signature) to match, the expert system will likely not accept this as a match, since the video key sub-signature should also have matched. The match probability is determined in the course of keyword and match word selection, as described below.

15. Number of sub-signatures—this number represents the number of sub-signatures which the key signature generation module has generated for a respective segment. In certain situations, as previously mentioned, the key signature generation module may generate multiple signatures (or sub-signatures) for a particular segment if this will increase the likelihood of obtaining more acceptable matches. For example, if the first key sub-signature produced has a low false match probability as well as a low probability of a true match, the module **410** may generate further sub-signatures for the segment to increase the probability of a true match. If so, in generating each further sub-signature the module **410** excludes frame signatures from runs previously used to generate key sub-signatures. However, if the false match probability of the first key sub-signature is comparatively high, further sub-signatures are not generated as that would increase the possibilities for a false match. In addition, if the module **410** determines that the false match probability for a video sub-signature is very high, it may choose not to generate any video sub-signatures. In a preferred embodiment, the key signature generation module may generate up to four key audio and video sub-signatures.

16. Expected peak width—typically, both keywords and matchwords are selected from the middle of frame signature runs. Accordingly, the segment recognition subsystem **26** may detect multiple matches on a given key signature for consecutive frames. The number of such consecutively detected matches is referred to as the peak width. The key signature generation module examines the run structure in the segment signature and generates an anticipated peak width value therefrom.

As previously described, each frame of an incoming segment has a frame signature associated therewith. The key signature generation module examines each of these frame signatures to select an acceptable keyword and eight matchwords for a respective key signature. In making such a selection, the key signature generator module **410** employs the following criteria:

1. Distribution of the selected frame signatures—the matchwords should be selected from among frame signatures which are evenly distributed throughout the segment signature. Such selection reduces the likelihood of false matching. For example, if two or more commercials have similar scenes, selecting matchwords from among evenly distributed frame signatures tends to cause at least several of the matchwords to be selected from frame signatures which lie outside of the similar scenes. The distribution of the matchwords is quantized as a normalized separation in time or frame intervals therebetween. However, signatures from frames near the ends of the segment should be avoided to ensure that the runs from which they are selected are contained within the respective segment, as well as to avoid utilizing signals which are more prone to variations in signal level (for example, due to the inherent delays in automatic gain control). Moreover, keywords are preferably selected from frames near the beginning of the segment, in order to maximize the available time for the expert system to evaluate a match on the corresponding key signature. Both keywords and match words should be selected from signatures at or near the centers of runs; this consideration is implemented by the match probability criterion in the manner described below.
2. The likelihood of a particular frame signature value being generated—the frame signatures generated by the segment recognition sub-system **26** may not be evenly distributed among all possible values of frame signatures, but instead may be clumped with other similar frame signatures. This corresponds with the a priori distribution of frame signatures discussed above in connection with the match rules and is determined by collecting statistically large numbers of frame signatures and determining their overall distribution to determine a normalized probability of generation for each potential frame signature. Clumping of frame signatures may cause false matching to occur and significantly increases the correlator processing load. As a result, in selecting frame signatures, the key signature generation module favors frame signatures which are not so clumped as compared to a clumped frame signature, thereby minimizing the number of key signatures having matchwords with similar values.
3. The distribution of previously established keywords—the key signature generator module **410** considers the distribution of keywords which have been previously generated and stored in a database of the segment recognition subsystem **26**. As an example, for a particular keyword, the key signature generation module considers the number of generated key signatures which are associated with this keyword. If such a keyword is already associated with a large number of key signatures, such keyword is less likely to be selected as compared to a keyword associated with a lesser number of key signatures. Thus, this factor, like factor **2** above is utilized for minimizing clumping to reduce the number of false matches which occur and to reduce correlator processing load. However, unlike the above factor **2**, this factor is dependent upon the broadcast signals. For example, if several commercials having similar data content are received, then several key signatures may be generated which have identical keywords. This is not due to the segment recognition subsystem **26**, unlike the above factor **2**, but is a function of the broadcast data and is determined as a normalized frequency of occurrence. Factors **2** and **3** are multiplied to yield a single factor indicating the undesirability of a given keyword due to clumping.
4. Run length—it has been observed that relatively short runs, for example, those having lengths less than approximately five frames, are less likely to match as compared to longer runs. Further, it has also been observed that the probability of having an acceptable match does not significantly increase for relatively long runs, for example, those having a length longer than approximately ten frames. However, such relatively long runs may produce key signatures having a relatively low entropy. Thus, it is desirable to utilize run lengths which are neither relatively short nor relatively long. In the preferred environment, the key signature generation module utilizes runs which have a length from approximately five to ten frames. Accordingly, a normalized figure of merit is assigned to each run length based on the foregoing criteria.
5. Match probability—once runs of acceptable length have been defined, the key signature generator module **410** assesses the probability of the frame signatures each successfully matching during a rebroadcast of the corresponding segment in accordance with the keyword matching process. More specifically, the keyword is selected as the frame signature at an offset n of the segment most likely to match upon rebroadcast of the segment within a predetermined guardband of ±g frame signatures. If the probability of a match with a frame signature at offset m in accordance with the keyword matching procedure (that is, a match of all 16 bits or of at least 15 of the 16 bits) is termed pk(m, n), then the probability pk(m, n) may be determined as follows:

$$pk(m,n)=15*PM+\Sigma[PM/F(i)],\ i=1 \text{ to } 15$$

where PM is the probability of a match on all bits deter-

mined as follows:

$$PM=\text{product } [P(i)],\ i=0 \text{ to } 15,$$

and P(i) is the probability of a match of bits (i) of the potential key word and frame signature, where i=0 to 15. It is appreciated that P(i) is determined on the basis of the respective mask bits of the potential keyword and the frame signature being compared.

It is further appreciated that the probability that a potential keyword at offset n will match with one or more frame signatures along a given interval from an offset a to an offset b, termed pk(a:b, n) may be derived from the relationship:

$$pk(a:a+1,n)=pk(a,n)+pk(a+1,n)-[pk(a,n)*pk(a+1,n)].$$

By induction, it is seen that:

$$pk(a:b,n)=pk(a:b-1,n)+pk(b,n)-[pk(a:b-1,n)*pk(b,n)],$$

which readily permits a determination of the probability that a given potential keyword at offset n will match with at least one frame signature over the interval ±g, termed pk(n−g: n+g, n). An advantageous technique for determining the guardband ±g calculates pk(n−g: n+g, n) for values of g increasing from zero until either pk(n−g, n) or pk(n+g, n) is below a predetermined threshold, which ensures that potential keywords near the centers of runs are advantageously accorded higher probabilities than those nearer the ends of the runs. By determining the respective such probabilities for all potential keywords among the acceptable runs of the segment signature, each potential keyword is assigned a figure of merit based on the matching probability determined in the foregoing manner.

Relative figures of merit are also assigned to potential match words which may be selected from the frame signatures of the acceptable runs. The figure of merit is determined in accordance with the manner in which the match words are utilized in the matching process, namely, the number of bits of each potential match word at offset n which are expected to match with the frame signatures at respective offsets m within the corresponding run are determined and then averaged over the run to derive an average number of bits expected to match over the run as the figure of merit. The number of bits expected to match between a potential match word at offset n and a frame signature at offset m, termed bm(m, n), is determined as follows:

$$bm(m,n)=\Sigma[P(i)],\ i=0 \text{ to } 15$$

where P(i) is the probability of a match of bits (i), obtained in the same manner as in the case of the keyword matching probability determination. Then the average of the number of bits expected to match, bm(m, n), is determined over a run length from offset a to offset b as follows:

$$bm(a:b,n)=\Sigma[bm(m,n)]/(b-a+1),\ m=a \text{ to } b.$$

The boundaries a and b of the run are determined in the same fashion as in the keyword matching probability determination.

6. Entropy—the key signature generation module prefers matchwords from the segment signature which have a relatively high entropy, that is, matchwords each having a respective data content which is dissimilar from that of the other selected matchwords. The selection of high entropy matchwords minimizes the correlation between matchwords and, consequently reduces the likelihood false matching. A normalized dissimilarity in data content among matchwords may be determined by counting the number of bits which are different between the matchwords.

7. Run sharpness—the key signature generation module preferably selects a keyword and the eight matchwords from within frame runs which are bounded by frame signatures having signature values which are substantially different than those of adjacent frames within the run. The difference in bit values between the boundary frame signature and adjacent signatures within the run is used to derive a normalized figure of merit for run sharpness.

It is appreciated that it may not always be possible to optimize each of the above seven factors when selecting a keyword and/or matchwords. Accordingly, for each keyword and/or matchword being considered, the key signature generation module assigns a normalized merit value for each of the above-described seven factors as described above. For keyword selection, respective keyword weighting factors are obtained from a parameter file and are multiplied with corresponding normalized merit values. The products are then summed to yield on overall merit value for each possible keyword. For matchword selection, the same process of weighting and combining the normalized factors of merit is employed, utilizing different respective weighting factors from the parameter file.

The parameter files are derived empirically. In accordance with one technique for doing so, all weighting factors are initially set to the same value and key signatures are then generated to evaluate the relative importance of each criterion in key signature generation. This process is repeated until by accumulation and evaluation of the results, the most advantageous weighting factors are ascertained. Different parameter files are maintained for video and audio signatures in recognition of their differing characteristics. The parameter files also include maximum allowable values for error thresholds as a function of segment length, as it has been observed that relatively short segments, for example, those shorter than approximately 10 seconds, are more likely to false match than relatively longer segments, for example, those of 30 seconds or more.

The basic steps utilized by the key signature generation module are illustrated in FIGS. **18**. As shown therein, frame signatures from defined runs which are under consideration for use as keywords and matchwords are obtained as shown in steps **S200** and **S210**, respectively. Thereafter, in **S220**, the most acceptable keyword and matchwords are selected by comparing the total merit values for each keyword and matchword candidate, as described above together with absolute criteria such as observance of maximum allowable error thresholds. From the selected keyword and matchwords, a corresponding key signature is created as indicated in step **S230**. Thereafter, in step **S240**, a determination is made whether more key signatures should be produced to increase the probability of matching. If the determination at step **S240** is affirmative, additional key signatures are produced by repeating steps **S200**–**S230**, utilizing different runs, however. If, on the other hand, additional key signatures are not required, as indicated by a NO at step **S240**, then the match rules for the key signature generated in step **S230** are formulated and combined with the key signature, as indicated in step **S250**.

Referring again to FIG. **17**, typical signal data flows in the generation of a key signature are illustrated therein. The signal data flow is primarily between the segment recognition subsystem **26** and the control computer **30**. More specifically, a desired broadcast signal is received by a respective one of the converters **24**, which is tuned to the

desired channel. Baseband video and audio signals are supplied from the tuner **24** to the corresponding one of the channel boards **402** of the segment recognition subsystem **26** which is adapted to generate frame signatures and corresponding mask words for each frame of the received baseband signals. These frame signatures and mask words are supplied to the segment recognition controller **404** of the segment recognition subsystem **26**.

Before it can be determined that a new segment of interest has been received so that a key signature must be produced, the segment recognition controller **404** attempts to match the received frame signatures with existing key signatures, as previously described. The segment recognition controller **404** supplies cues (including match reports) to the expert system module **414** contained within the control computer **30** which the expert system uses to detect new segments of interest. Thereafter, the expert system **414** supplies a request signal to the segment recognition controller **404** for the segment signature of the segment which did not match and which may be a new segment of interest. In response thereto, the segment recognition controller **404** retrieves the respective segment signature from a segment signature ring buffer **406** and supplies the same to the expert system module. If the expert system **414** determines that the respective segment is a segment of interest, the expert system supplies a signal, which includes all necessary information pertaining thereto (e.g., the segment signature, an identification number, the channel and the time of day), through the database control module **416** to the key signature generator **410** implemented by the control computer **30**. The key signature generator **410** generates a new key signature for the received segment in a manner as previously described and supplies the new key signature through the database control module **416** to the segment recognition controller **404** which, in turn, supplies the same to a key signature database **408**. Further, information regarding the new segment of interest is supplied from the database control module **416** to the database **412**.

The term "probability" as used throughout this specification refers both to the relative likelihood or frequency of occurrence of an event or events as well as the absolute likelihood of an event or events occurring, and may be expressed either as a normalized value or otherwise, for example, as an unquantified expression of the relative likelihood of two or more events. The term "broadcast" as used herein refers to various modes for the wide dissemination of information, such as radio and television broadcasts, whether distributed over-the-air, by cable, CATV, satellite or otherwise, as well as other modes for the wide dissemination of data and information.

It is appreciated that, while video frame or field intervals are utilized in the disclosed embodiment for the generation of signatures as well as for other purposes in connection with a television commercial recognition system, the use of frame or field intervals is employed merely for convenience, and it is understood that different intervals may be selected for signature generation and such other purposes. As an example, signatures may be produced from a combination of fields or frames or from subsets of frame or field information in video signals, and that audio intervals need not correspond with video intervals, but may be arbitrarily chosen. In accordance with a system for recognizing radio broadcast segments, any arbitrary interval may be utilized for signature generation and other purposes, provided that sufficient information is included in the selected interval.

While an embodiment of the present invention has been disclosed for recognizing television broadcast commercials, it will be understood that the systems and methods for continuous pattern recognition of broadcast segments in accordance with the present invention may be utilized for other purposes, such as determining what programs, songs or other works have been broadcast, for example, for determining royalty payments, or else for determining the programs, commercials or other segments which have been received by audience members participating in an audience measurement survey.

It will be appreciated that the systems and methods of the present invention may be implemented in whole or in part using either analog or digital circuitry, or both, and that the elements and steps thereof may be implemented or carried out utilizing any of a variety of system and subsystem configurations and devices, and that the various steps and elements may be carried out and implemented either with the use of hardwired or software based processors.

Although specific embodiments of the invention have been described in detail herein with reference to the accompanying drawings, it is understood that the invention is not limited to those precise embodiments, and that various changes and modifications may be effected therein by one skilled in the art without departing from the scope or spirit of the invention as defined in the appended claims.

We claim:

1. A method for selectively capturing at least one of a broadcast audio signal and a broadcast video signal for use in updating a broadcast segment recognition database storing signatures for use in recognizing broadcast segments of interest, comprising the steps of:

temporarily storing at least one of a broadcast audio signal and a broadcast video signal of a monitored broadcast;

detecting predetermined signal events indicating possible new broadcast segments of interest of the monitored broadcast;

selecting intervals of the monitored broadcast as possible new broadcast segments of interest based upon said predetermined signal events;

assigning a first capture level to a first selected interval based on predetermined characteristics thereof indicating that said first selected interval is likely to be a new segment of interest;

assigning a second capture level to a second selected interval based on predetermined characteristics thereof indicating that the second selected interval is relatively less likely than the first selected interval to be a new segment of interest;

storing a signature corresponding with the first selected interval in the database and capturing at least one of the temporarily stored broadcast audio and video signals corresponding with the first selected interval for transmission to a workstation operator for segment identification;

storing a signature corresponding with the second selected interval in the database; and

erasing the temporarily stored one of the broadcast audio and video signals corresponding with the second selected interval.

2. The method of claim **1**, further comprising the steps of detecting a match of the stored signature representing the second selected interval with a signature representing a subsequently received segment, and capturing at least one of audio and video data of the subsequently received segment for transmission to the workstation operator for new segment recognition.

3. A system for selectively capturing at least one of a broadcast audio signal and a broadcast video signal for use in updating a broadcast segment recognition database storing signatures for use in recognizing broadcast segments of interest, comprising;

means for temporarily storing at least one of a broadcast audio signal and a broadcast video signal of a monitored broadcast;

means for detecting predetermined signal events indicating possible new broadcast segments of interest of the monitored broadcast;

means for selecting intervals of the monitored broadcast as possible new broadcast segments of interest based upon said predetermined signal events;

means for assigning a first capture level to a first selected interval based on predetermined characteristics thereof indicating that said first selected interval is likely to be a new segment of interest;

means for assigning a second capture level to a second selected interval based on predetermined characteristics thereof indicating that the second selected interval is relatively less likely than the first selected interval to be a new segment of interest;

means for storing a signature corresponding with the first selected interval in the database and capturing at least one of the temporarily stored broadcast audio and video signals corresponding with the first selected interval for transmission to a workstation operator for segmented identification;

means for storing a signature corresponding with the second selected interval in the database; and

means for erasing the temporarily stored one of the broadcast audio and video signals corresponding with the second selected interval.

* * * * *

US005764770A

United States Patent [19]

Schipper et al.

[11] Patent Number: 5,764,770

[45] Date of Patent: Jun. 9, 1998

[54] **IMAGE AUTHENTICATION PATTERNING**

[75] Inventors: **John F. Schipper**, Palo Alto; **Allan M. Pelley**, Milpitas, both of Calif.

[73] Assignee: **Trimble Navigation Limited**, Sunnyvale, Calif.

[21] Appl. No.: **905,842**

[22] Filed: **Aug. 4, 1997**

Related U.S. Application Data

[63] Continuation of Ser. No. 554,511, Nov. 7, 1995, abandoned.

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/25**; 380/54

[58] **Field of Search** 380/20, 21, 23–25, 380/54; 382/209

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,798,360	3/1974	Feistel .	
3,872,483	3/1975	Numata et al. .	
3,882,512	5/1975	Lawrence et al. .	
3,968,505	7/1976	Kanneckas et al. .	
4,053,240	10/1977	Aizawa et al. .	
4,064,515	12/1977	Mashimo et al. .	
4,074,324	2/1978	Barrett .	
4,122,521	10/1978	Rick et al. .	
4,131,919	12/1978	Lloyd et al. .	
4,149,795	4/1979	Sakurada et al. .	
4,175,848	11/1979	Murakami et al. .	
4,361,388	11/1982	Micak et al. .	
4,405,829	9/1983	Rivest et al.	380/30
4,418,425	11/1983	Fennel et al. .	
4,489,351	12/1984	Arc .	
4,541,010	9/1985	Alston .	
4,626,898	12/1986	Baba et al. .	
4,635,203	1/1987	Merchant .	
4,680,628	7/1987	Wojcik et al. .	
4,695,959	9/1987	Lees et al. .	
4,702,585	10/1987	Harada et al. .	
4,704,632	11/1987	Van Den Heuvel .	
4,709,266	11/1987	Hanas et al. .	
4,837,628	6/1989	Sasaki .	
4,860,352	8/1989	Laurance et al.	380/23
4,887,296	12/1989	Horne	380/20
4,916,737	4/1990	Chomet et al. .	
4,993,067	2/1991	Leopold .	
5,045,937	9/1991	Myrick .	
5,115,467	5/1992	Esserman et al. .	
5,191,613	3/1993	Graziano et al. .	

(List continued on next page.)

OTHER PUBLICATIONS

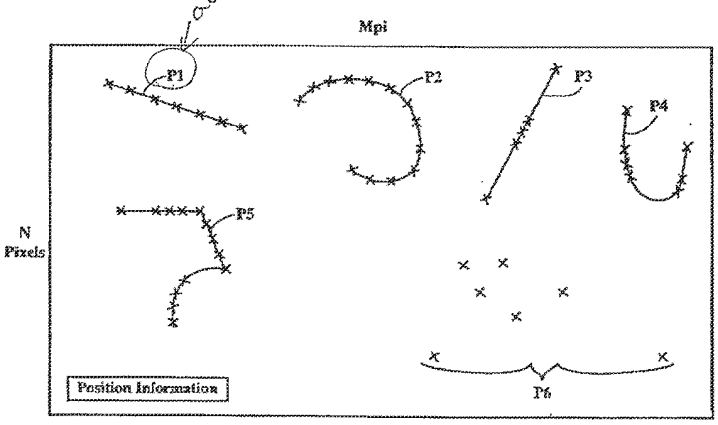
S. Walton, "Image Authentication for a Slippery New Age," Dr. Dobb's Journal, Apr. 1995, pp. 18–26.

Primary Examiner—Salvatore Cangialosi
Attorney, Agent, or Firm—John F. Schipper

[57] **ABSTRACT**

Apparatus for producing a self-authenticating visual image of a selected view, using a digital image forming means, such as a digital camera, together with a position determining system that provides position information, including location and/or angular orientation and/or time of observation at the time a digital image is formed. The digital image of the selected view is presented as an array of pixels with associated pixel values. The position information is incorporated in the digital image by altering selected pixel bit values for a selected authentication pattern P of pixels in a chosen subset CS of the pixel array; and this selected pattern may be determined using the position information. The position information may be encrypted, using an encryption key based on position information, and may be stored separate from, or as part of, the digital image. The authentication pattern is represented by an authentication key or indicium, a single number or an ordered sequence of numbers, that is transmitted with the modified digital image and incorporated position information. The authentication pattern P is preferably chosen so that any circle or other connected pixel region of diameter at least equal to a selected number D contains at least one pixel from the subset CS. The pixel array may be overlaid by a set of polygons, such as triangles, rectangles, parallelograms or hexagons, with at least one pixel from the subset CS in each polygon.

34 Claims, 17 Drawing Sheet



U.S. PATENT DOCUMENTS

5,221,925	6/1993	Cross .	
5,237,612	8/1993	Raith .	
5,243,652	9/1993	Teare et al.	380/21
5,247,575	9/1993	Sprague et al. .	
5,296,884	3/1994	Honda et al.	354/106
5,321,753	6/1994	Gritton .	
5,347,580	9/1994	Molva et al. .	
5,348,529	9/1994	Goldfine et al. .	
5,349,459	9/1994	Reed .	
5,363,448	11/1994	Koopman et al. .	
5,379,224	1/1995	Brown et al. .	
5,382,957	1/1995	Blume .	
5,384,846	1/1995	Berson et al. .	
5,386,117	1/1995	Piety et al. .	
5,388,158	2/1995	Berson et al. .	
5,390,245	2/1995	Dent et al. .	
5,390,297	2/1995	Barber et al. .	
5,406,619	4/1995	Akhteruzza-man et al. .	
5,408,217	4/1995	Sanderford .	
5,440,301	8/1995	Evans .	
5,442,342	8/1995	Kung .	
5,451,757	9/1995	Heath .	
5,521,984	5/1996	Denenberg et al.	382/209 s

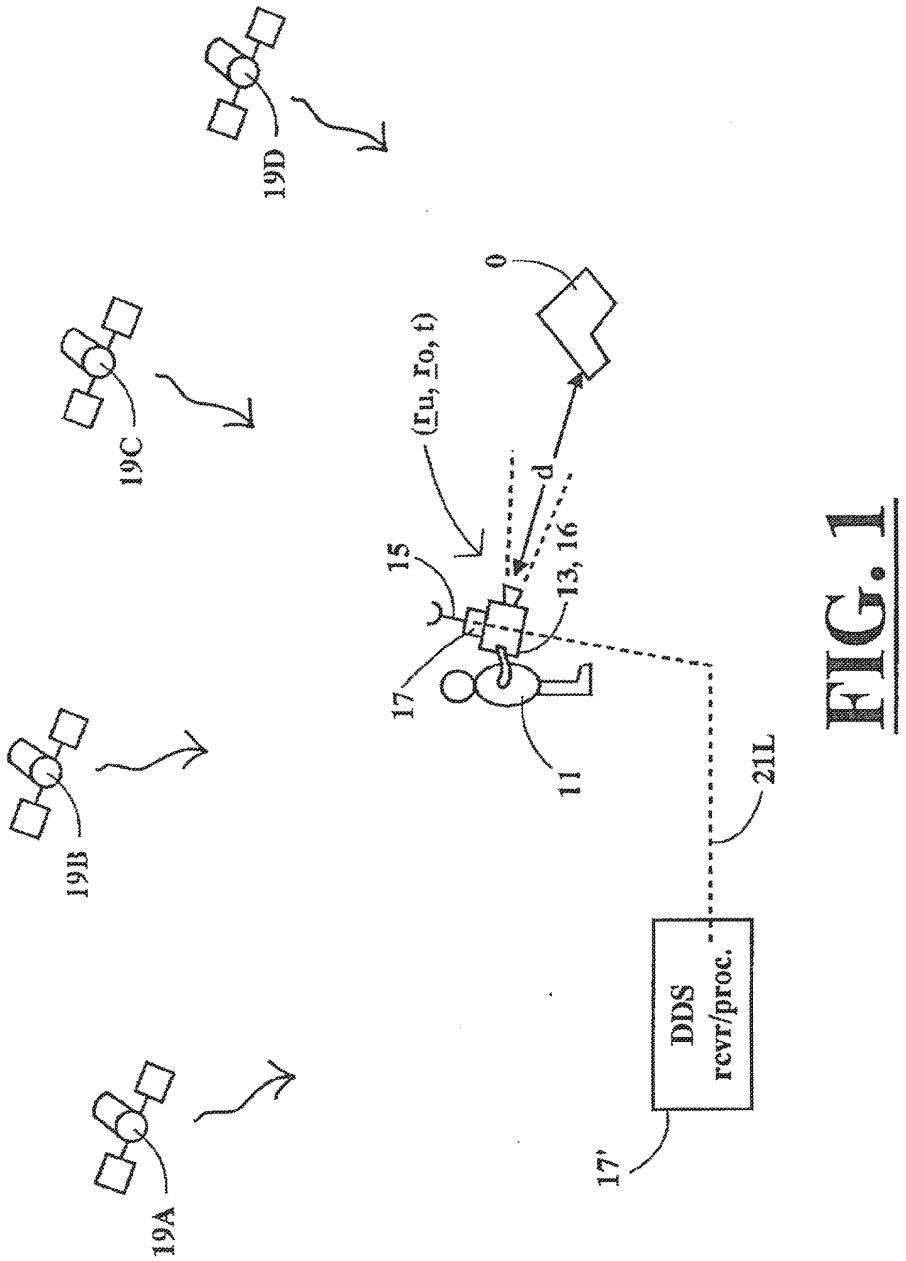


FIG. 1

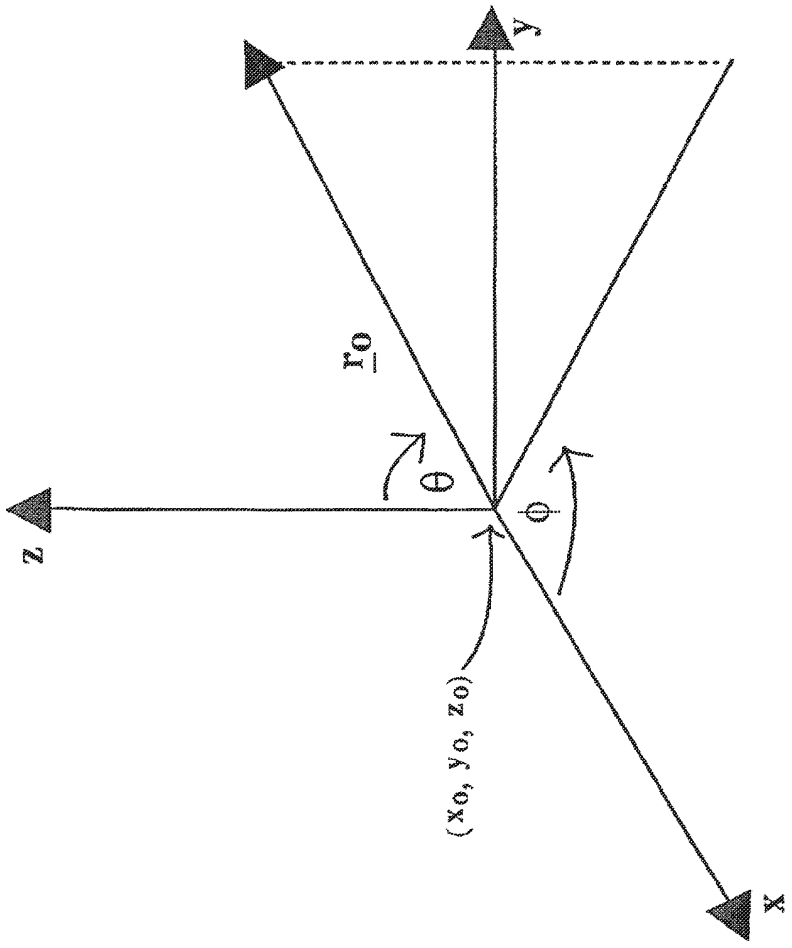


FIG. 2

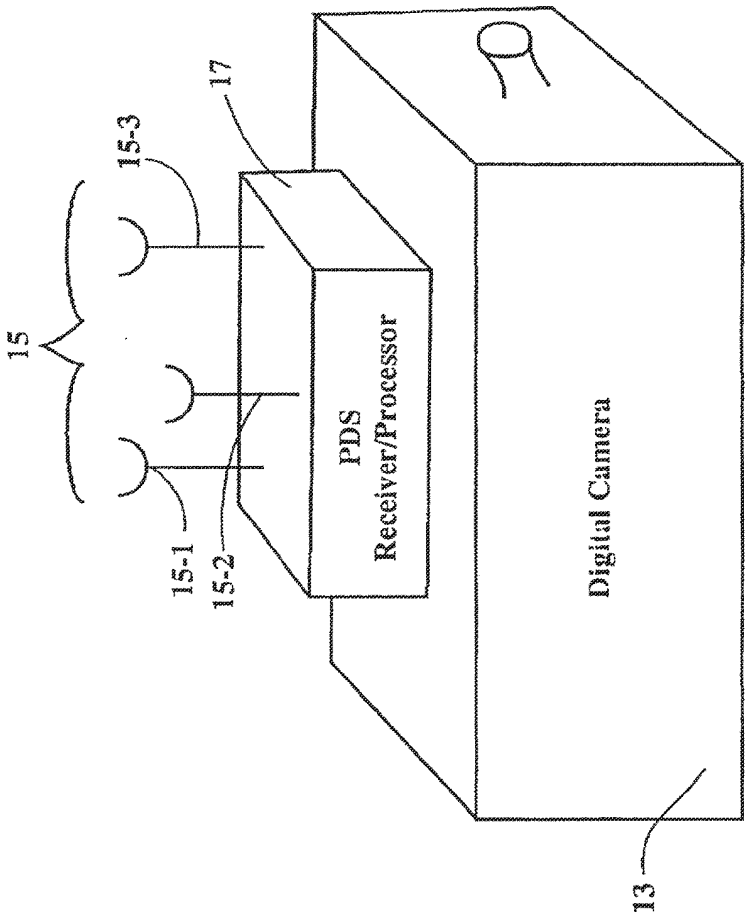


FIG. 3

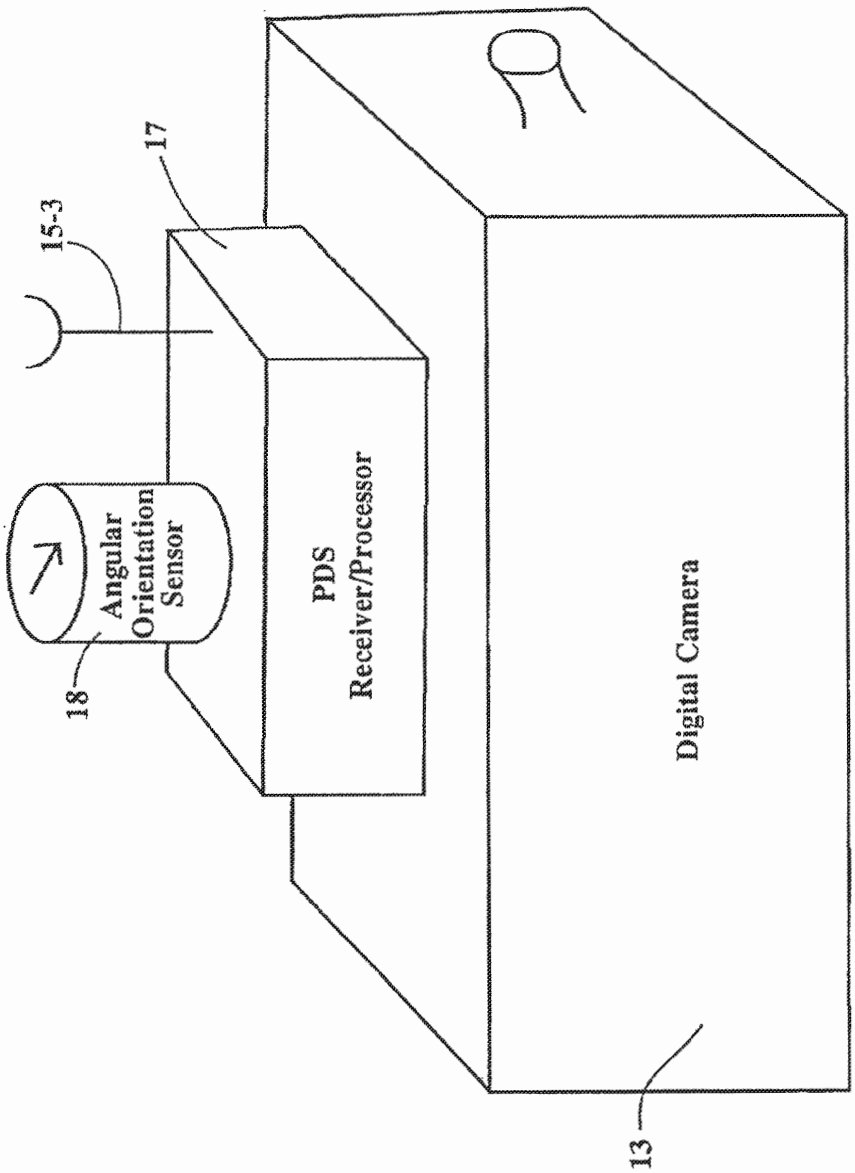


FIG. 4

ADOBE – Exhibit 1002, page 218

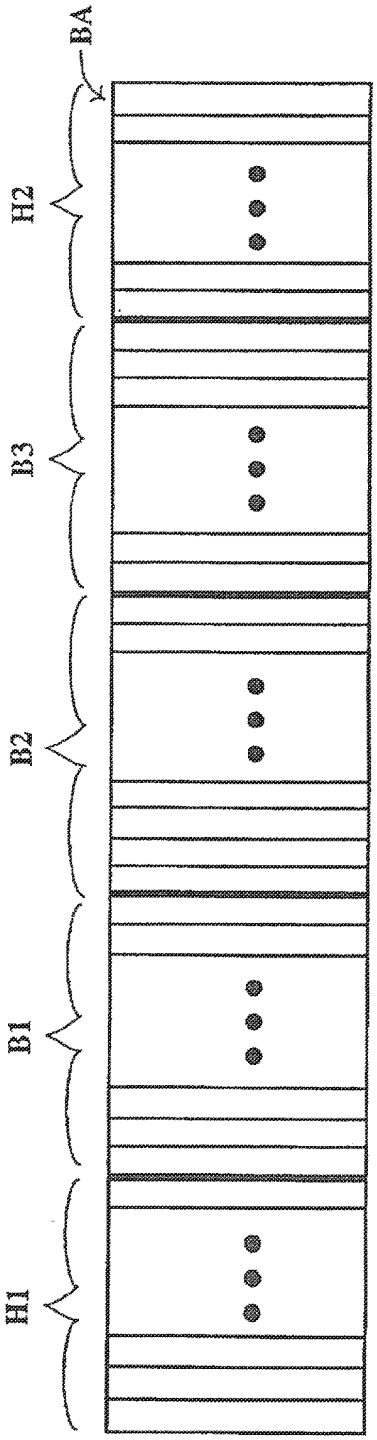


FIG. 5

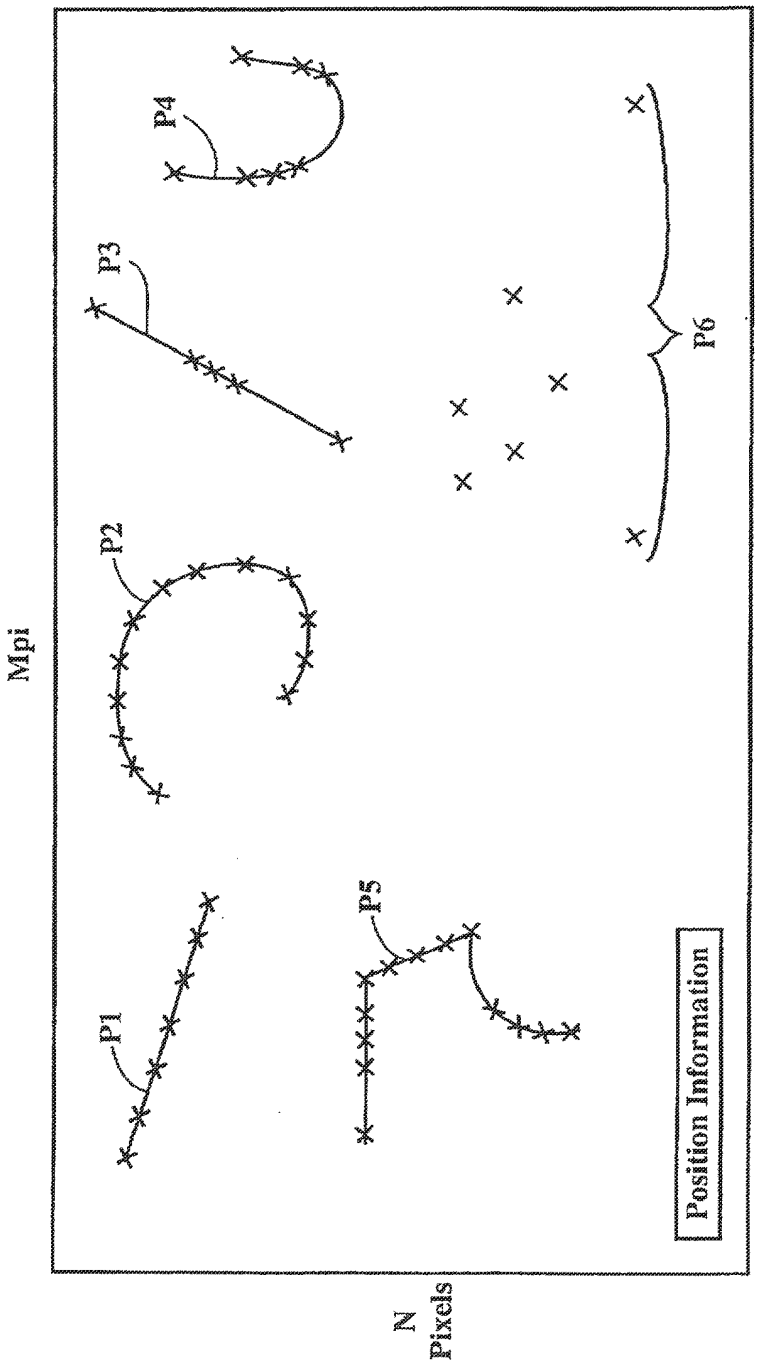


FIG. 6

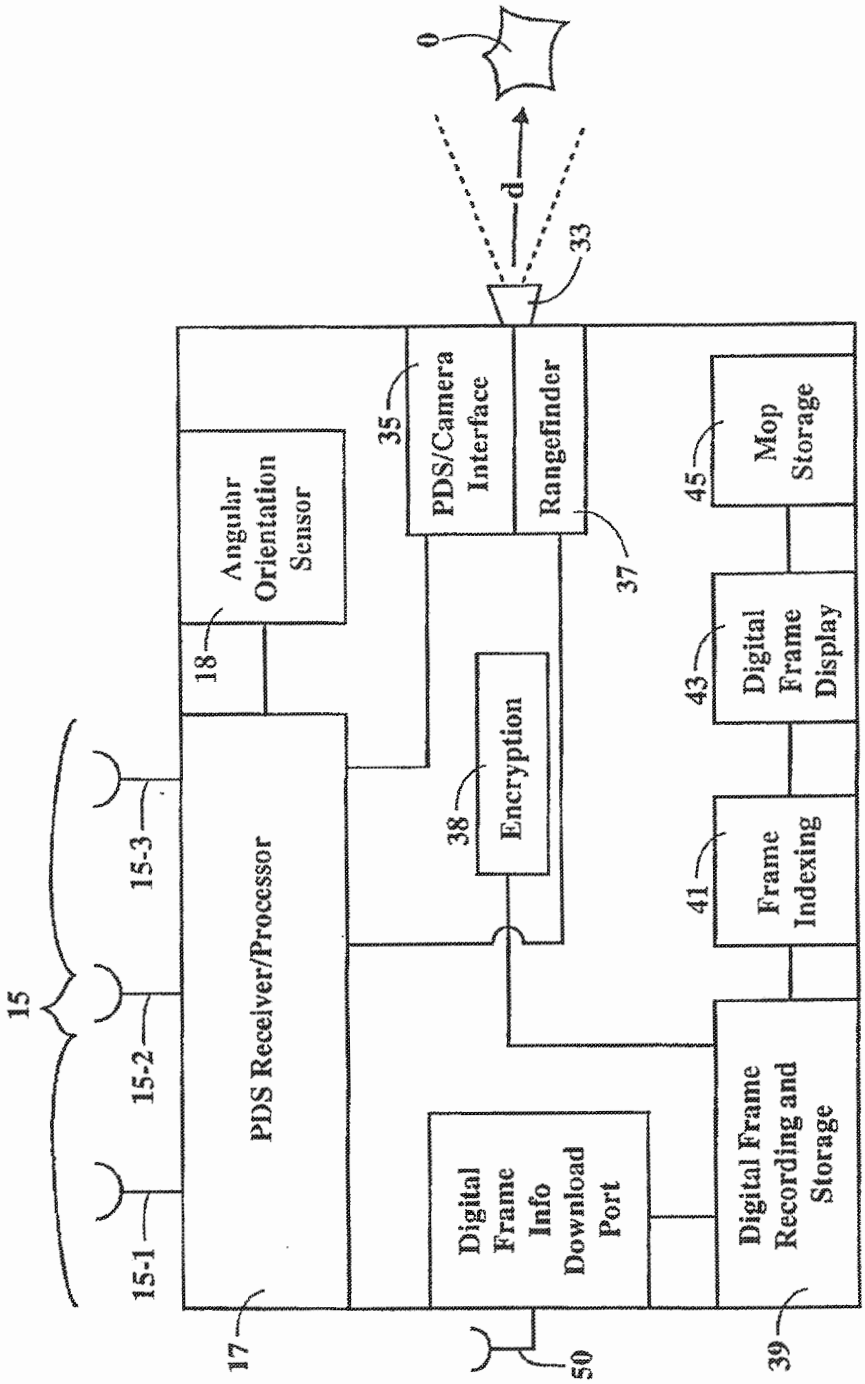


FIG. 7

ADOBE – Exhibit 1002, page 221

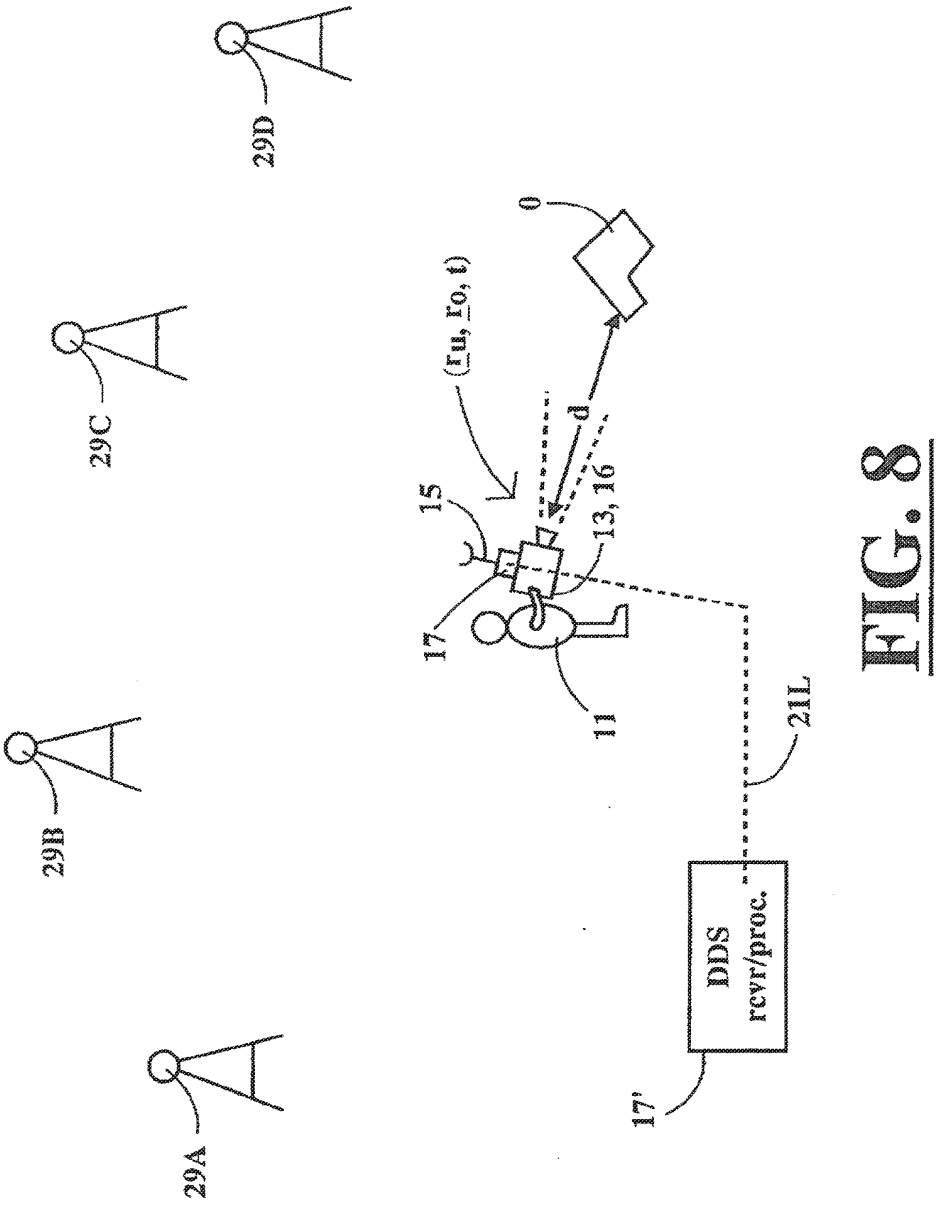


FIG. 8

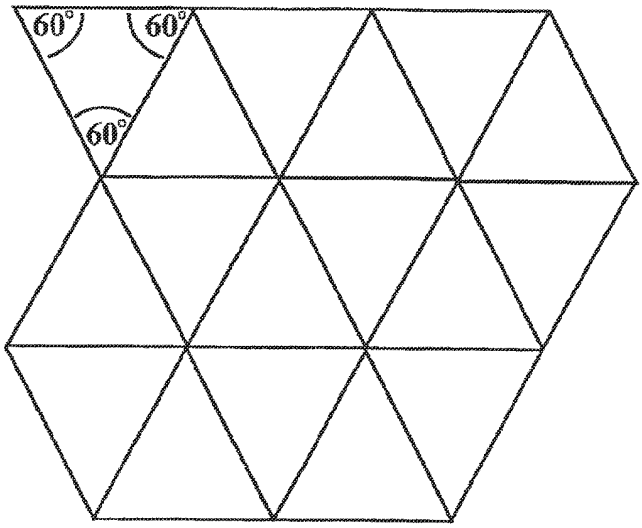


FIG. 9A

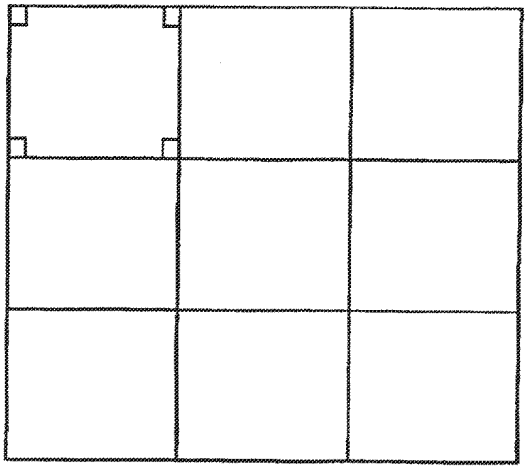


FIG. 9B

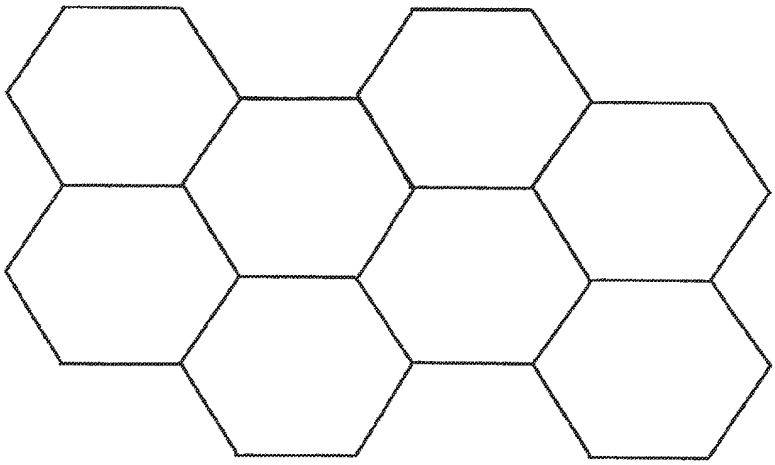


FIG. 9C

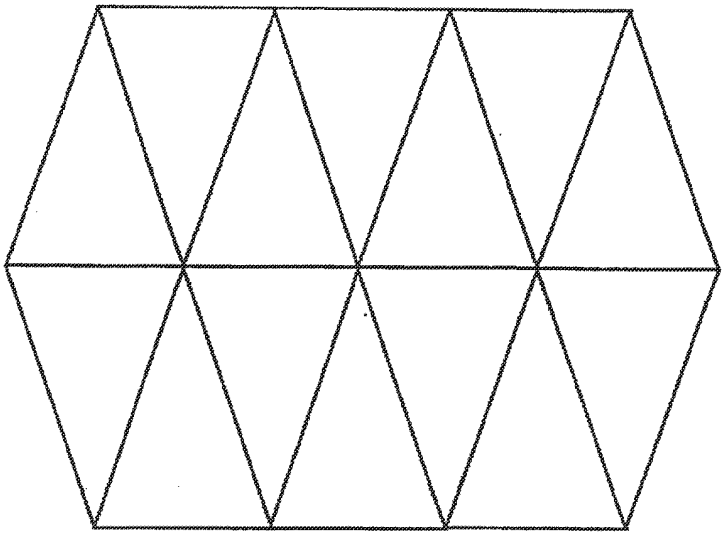


FIG. 9D

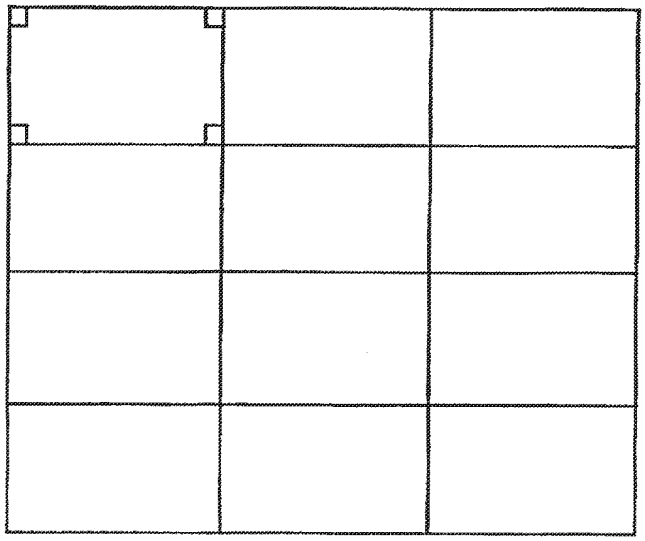


FIG. 9E

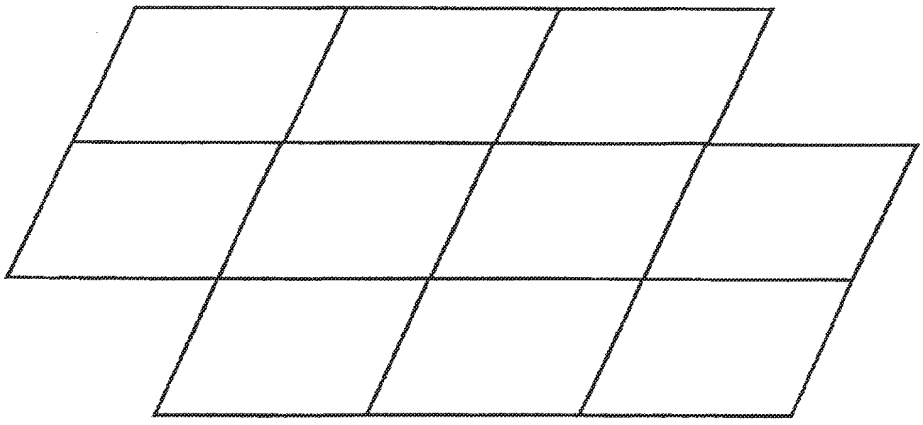


FIG. 9F

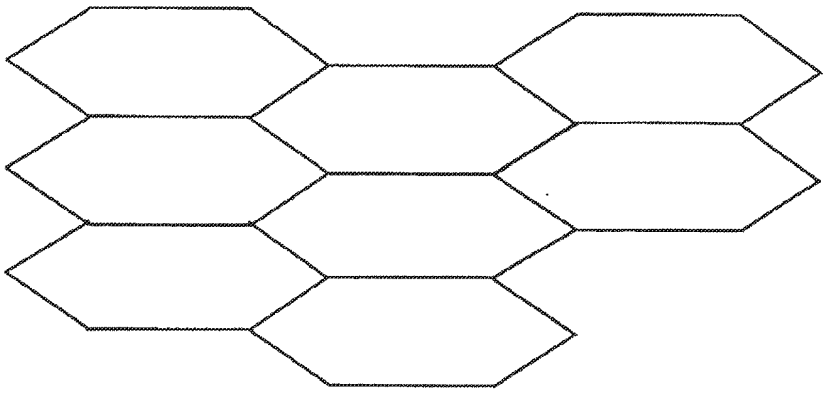


FIG. 9G

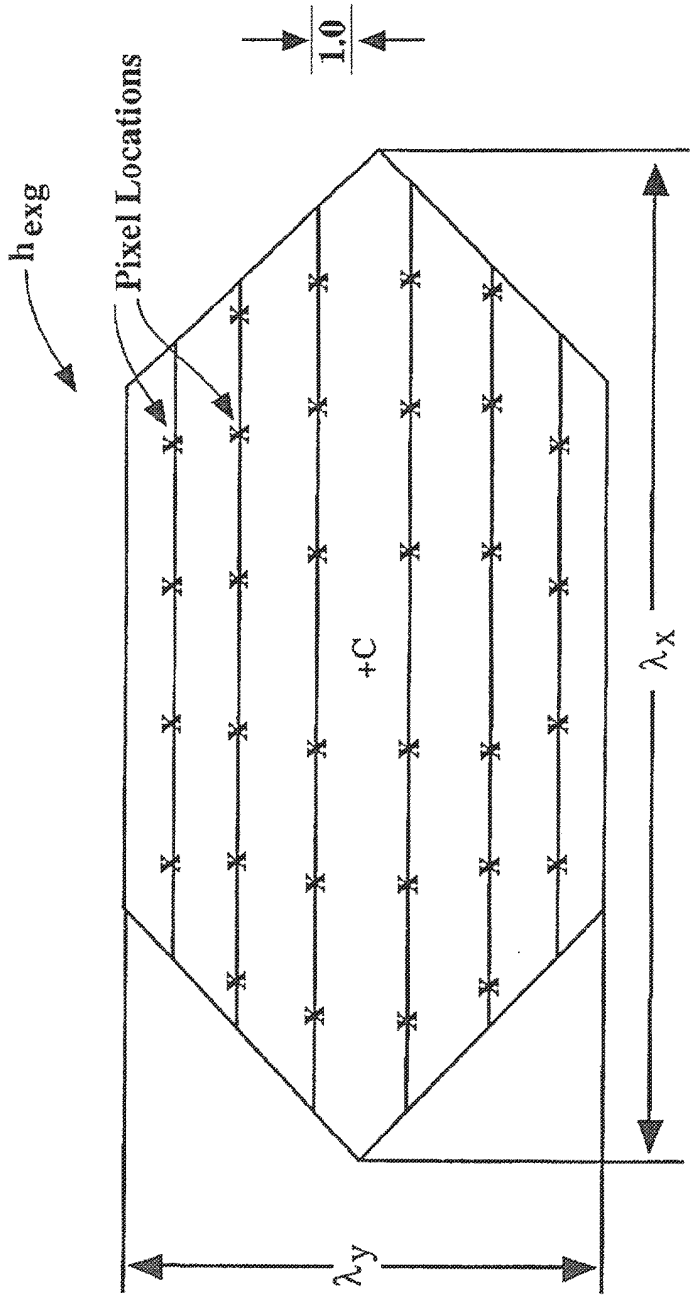


FIG. 10

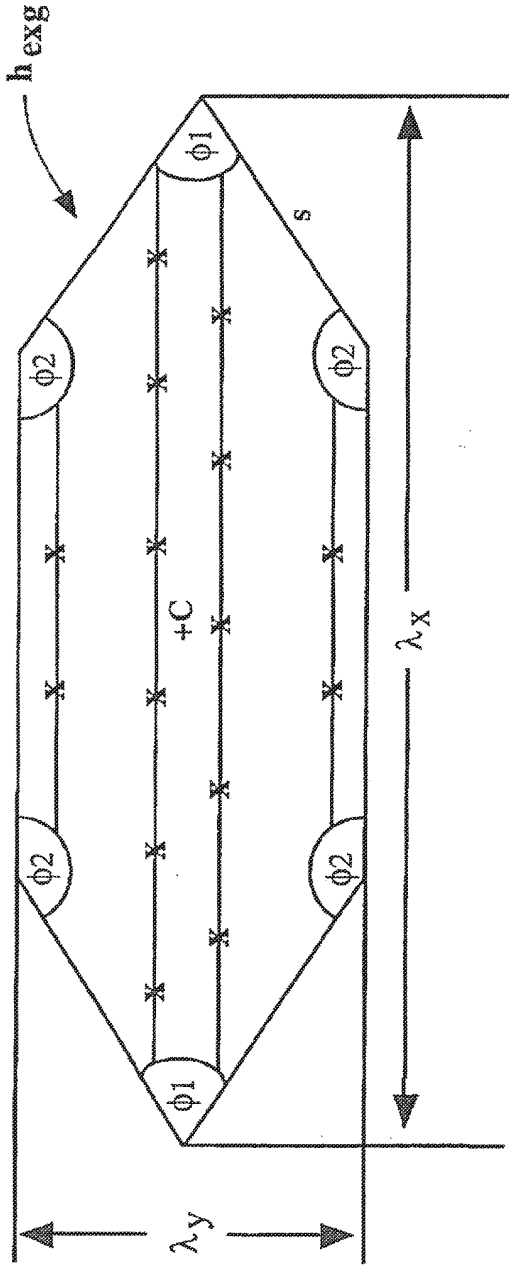


FIG. 11

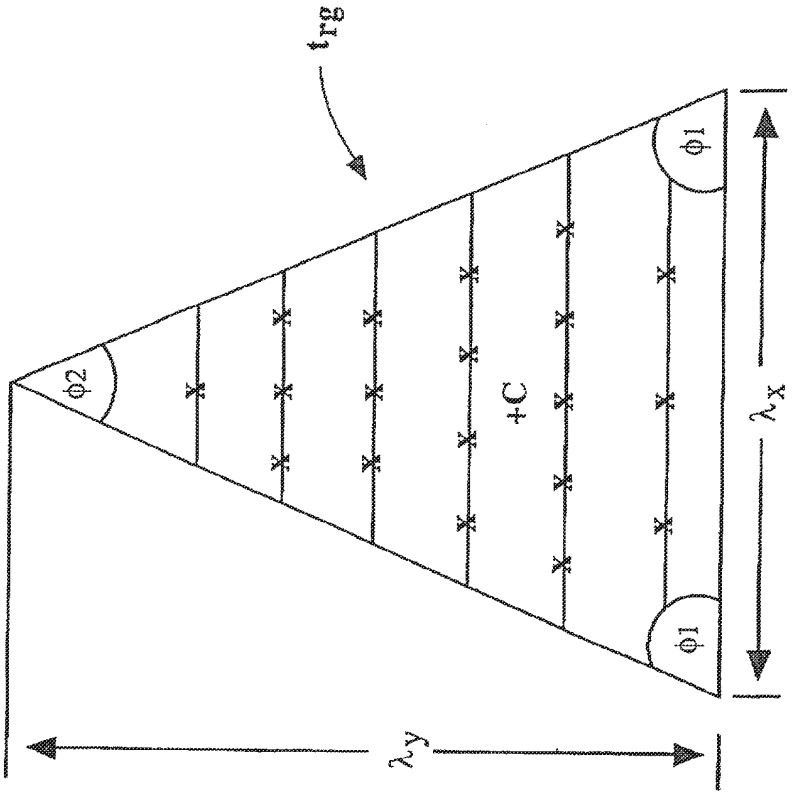


FIG. 12

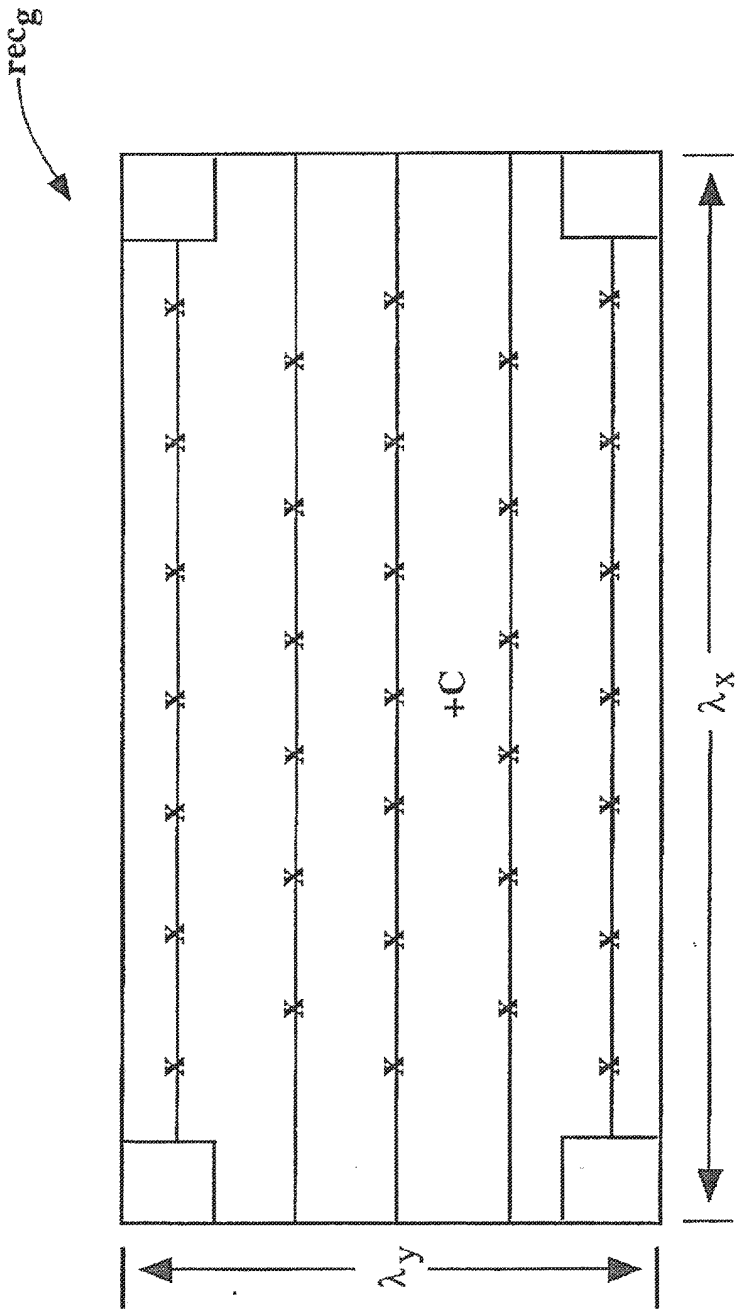


FIG. 13

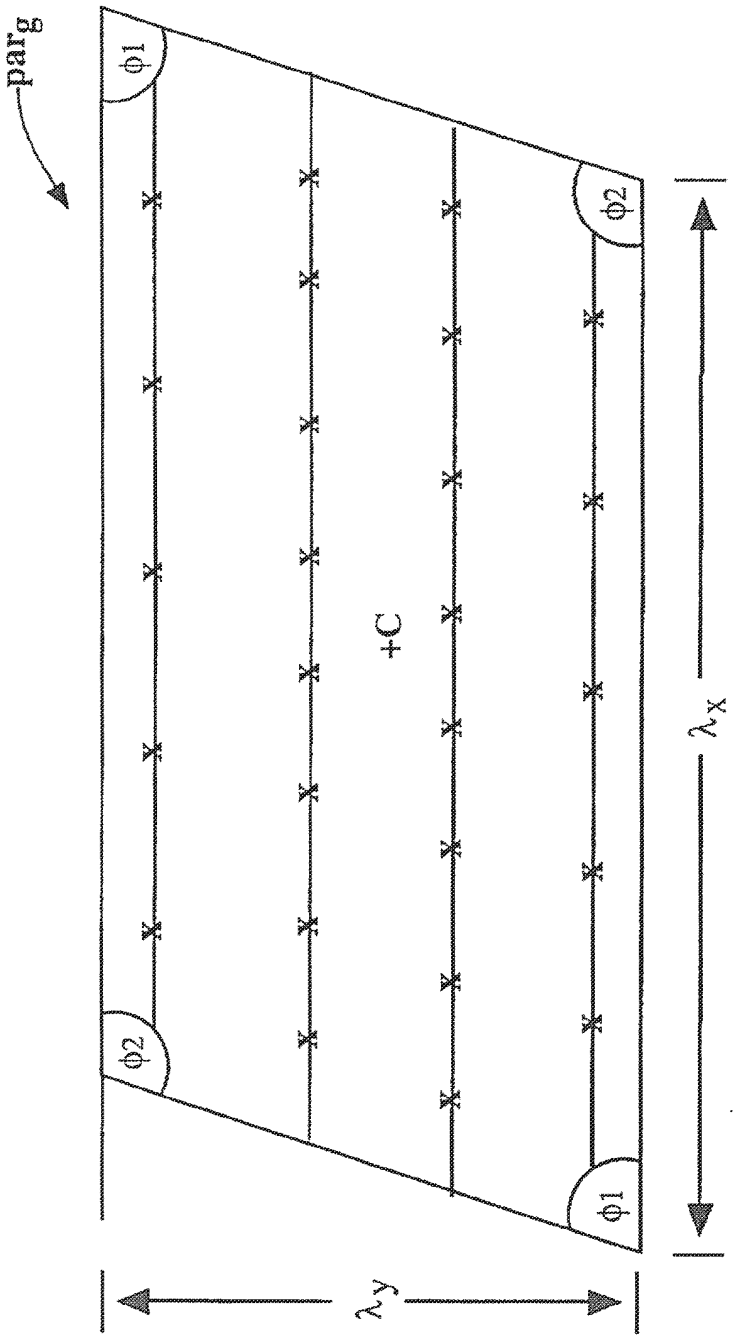


FIG. 14

IMAGE AUTHENTICATION PATTERNING

This application is a File-Wrapper Continuation of U.S. patent application entitled, "IMPROVEMENTS IN IMAGE AUTHENTICATION PATTERNING" Ser. No. 08/554,511 filed Nov. 7, 1995, now abandoned.

FIELD OF THE INVENTION

This invention relates to identification of the circumstances under which a visual image was formed, and authentication of the image.

BACKGROUND OF THE INVENTION

The parallel development of telecommunications and of computers over the last 25 years has allowed an awesome increase in data throughput and data analysis. Much of the business information that was once hand delivered by a known and trusted intermediary is now delivered electronically. For example, the Internal Revenue Service now encourages electronic filing of tax returns and related information and provides facilities for no-cost data transmission in some instances. Financial transactions, such as funds transfer and payment of invoices, are now routinely handled by electronic messaging. Electronic offices, both mobile and stationary, are now commonplace, along with cellular telephones, mobile facsimile machines and other accoutrements of this new age.

Unfortunately, this rise in computer power and data transmission power has brought an increase in the possibility of electronic mischief, unintentional and intentional, benign and injurious. A transmitter of an encrypted message is usually concerned with (1) delivery of the message only to its intended recipient(s) and (2) encryption of the message so that a message received by an unintended recipient cannot be decrypted to become privy to the intelligence contained in the message. However, the recipient of this message has somewhat different concerns, including a means of verifying that the message received was, in fact, transmitted by the putative sender. The message transmitter is concerned with secrecy and selectivity of the message recipients. The intended recipient is concerned with receiving and taking appropriate action only on messages for which the putative message source is the true or authentic source. If the putative source is not the actual source, the message may contain selective disinformation, intended to mislead the recipient or to cause the recipient to take action that the recipient would not otherwise take. For example, the Time magazine issue for 26 Jun. 1995, on page 65, reports some of the problems faced by Internet participants who are receiving fake e-mail messages, transmitted by someone other than the asserted sender of such messages.

Opto-electronic technology now allows a user to form an image using a digital camera, defined here to mean a visually perceptible image that is digitally expressed as an assembly of picture elements or pixels. Once an image is formed by opto-electronic means, the user may wish to include certain accompanying information indicating the circumstances under which the image was formed. If the image is to be used for some legal or related purpose, the user may wish to insure that the image or the accompanying information not be tampered with or corrupted.

Relatively few workers in electronic communications have seriously considered approaches for authenticating the putative source of information in the form of text or an image that is delivered electronically or by some means other than a trusted intermediary. Encryption using destination addresses using a TDMA satellite communications system is disclosed in U.S. Pat. No. 4,418,415, issued to Fennel et al. A common encryption/decryption key is held by all authorized users of a network. This key is EXclusively ORed with the specified destination address, and the output (digital) signal is passed through an encryption engine, on the satellite and at the intended ground-based receiver, using the same key or another key. The encryption engine output signal is then combined with the channel data to be transmitted in another EXclusive OR circuit and transmitted to the network users. Each of the receivers receives the message and reverses the encryption process, using its own destination address as part of the decryption key. However, only the (single) intended receiver produces a cleartext message that is comprehensible.

Hanas et al, in U.S. Pat. No. 4,709,266, disclose use of a satellite scrambling network to provide messages that are scrambled or encrypted differently for different geographical regions. This is useful for distributing scrambled video, voice and data subscriber messages. A master uplink message (ground-to-satellite) is used to control the scrambling or encryption commands that determine the scrambling applied to each geographical area and/or to groups of individual subscribers.

In U.S. Pat. No. 4,860,352, Laurance et al disclose a satellite communication system that provides authentication of a data transmission based upon the location of the data transmitter, as determined by the satellite communication system itself. The message sender transmits a message and the sender's location to a satellite, which retransmits the message and sender location to a ground-based receiver that compares the sender's stated location with the known location for the putative source of the message. Optionally, the message and/or the sender location are encrypted. If the two sets of transmitter location information agree, the message and its source are accepted as valid or authenticated. If the the two sets of such information do not agree, the receiver discards the remainder of this message as originating from an invalid sender. The message originator may be stationary or mobile. In one embodiment, a mobile message originator sends its present location and its location at the time the preceding message was sent, in encrypted text. A receiver receives the preceding location information and compares this with the known preceding location to verify or refute the preceding location of the putative source. In a second embodiment, three spaced apart satellites receive the same message and, based upon differences in time of receipt, determine the present location of the message originator. The message and this present location information are transmitted to a ground-based receiver, which compares the originator's present location with the known preceding location of the message originator, to verify or refute (within certain geographical limits) that the message originator is the putative source of the message. Some of the embodiments appear to require foreknowledge of the location, as a function of time, of the authentic message originator.

The inventors in the Laurance et al patent distinguish between (1) an "active attack," whereby an unauthorized person or the (faulty) transmission channel itself receives and alters the message and subsequently causes the message to be delivered to the recipient, and (2) a "passive attack," whereby an unauthorized person receives but does not alter the message that is delivered to the recipient. A third type of attack may be characterized as origination of a fraudulent message by a non-legitimate source, where the putative message source is not the actual message source. Active and passive attacks have traditionally been combated by mes-

sage encryption. Once the encryption method is broken and available for use by an unauthorized person, that encryption scheme is less than useless. Successfully combating an active attack and/or fraudulent origination requires more than message encryption: the message source must be authenticated and/or the received message must be verified as unaltered after its transmission by the putative source.

Horne, in U.S. Pat. No. 4,887,296, discloses a three-key cryptographic system for a direct broadcast satellite system, to be used in video broadcasting to a plurality of ground-based receivers, each having a unique address number. A signature key, which is an encryption using the address number for that receiver, is stored in the receiver at the time of manufacturing. At the transmitter, a common key is encrypted, using the unique signature key for a receiver that is targeted for a portion of the message to be transmitted. The data stream contains message portions intended for all receivers and message portions intended for, and decryptable only by, individual receivers. A target receiver decrypts its messages, using the common key and signature key used by the transmitter to encrypt the receiver's portions of the message.

U.S. Pat. No. 4,916,737, issued to Chomet et al, discloses an anti-piracy television program scrambling/descrambling system that allows the encryption/decryption code to be changed periodically (e.g., once per month) by communication from the head end or central station. The receiver's decryption unit has an unalterable ROM portion, containing its unique serial or address number, and an EPROM portion, containing an alterable ROM portion with a look-up table that can be changed by receipt of special signals from the head end.

U.S. Pat. No. 4,993,067, issued to Leopold, discloses a secure satellite-ground communication system that provides over-the-air encryption rekeying. A message transmitted from a proper ground station to the satellite must contain the ground station location. If the location of the ground station is not included in the message, or if this location is included but is not on an approved list maintained by the satellite, the received message is discarded. If the ground station location is acceptable, the satellite accepts the message and rekeys itself according to the rekeying information contained in the remainder of the message. This approach appears to require that the ground stations on the approved list be stationary.

Signal encryption apparatus that uses a common data key component and a specialized data key component, for a plurality of communicating sites, is disclosed in U.S. Pat. No. 5,115,467, issued to Esserman et al. The specialized data include distinct parameter values that are associated with only one communicating site. The encryption generating key depends upon the common data key component and upon the specialized data key component so that the encryption key used for each site may be distinguishable. The invention is useful in receipt and processing of television signals generated at a plurality of fixed sites.

Graziano et al, in U.S. Pat. No. 5,191,613, disclose a knowledge-based system for the electronic equivalent of signature authentication of a document, such as an agreement, transmitted from a sender to a recipient. The document, in electronic form, is temporarily locked into a computer memory so that no modifications can be made to the document or its format. Each of the document signatories then applies its own tests and comparisons to verify electronically that the document is authentic and unaltered. After this authentication process, each signatory affixes its electronically-based signature to the document to activate the terms of the agreement.

In U.S. Pat. No. 5,221,925, Cross discloses a location interrogation system in which a mobile unit, upon receipt of an interrogation signal, transmits its present location in a conventionally encoded format to a central station that has issued the interrogation signal, to assist in tracking the mobile unit.

A verification procedure for mobile stations in a cellular network is disclosed by Raith in U.S. Pat. No. 5,237,612. In response to receipt of a random challenge signal or interrogation, the mobile station transmits to the central station a first response signal, depending only upon an unchanging, commonly-held encryption key, and a second response signal, dependent upon a changeable encryption key. The first and second response signals are analyzed by an authentication algorithm to authenticate, or deny authentication to, the putative mobile station.

U.S. Pat. No. 5,243,652, issued to Teare et al, discloses a communication system for control of access to a location-sensitive remote database. A central station stores and transmits encrypted television material whose encryption key is available only for a viewers in a specified geographical area, as determined by a GPS or Loran location determination system. A secure version of the location history of the mobile user is transmitted to a central facility and compared with the known location history of this user. If the two histories agree, the identity of the user is confirmed, and a decryption key associated with this location history is transmitted to the user, for use in decrypting the encrypted television transmission.

Transmission of encrypted information packages from a central site to a remote site, in response to receipt of a request for specified information from that site, is disclosed in U.S. Pat. No. 5,247,575, issued to Sprague et al. The encryption key is changed periodically (e.g., weekly), but does not depend upon any past information.

Honda et al, in U.S. Pat. No. 5,296,884, discloses a camera that allows recording of location and/or time as a supplement to the frame image, where the location/time information is provided by signals received from a Loran, Decca, Omega or GPS signal source. The location/time information appears to be recorded separately from the camera image, perhaps on an adjacent strip of film. A similar device that uses earlier location-indicating instruments is disclosed by Rick et al in U.S. Pat. No. 4,122,521.

Earlier patents that allow recording of exposure information, exposure time/date, distance to a selected object in view, or local terrain detail, on film or in a viewfinder at the time a camera forms an image on the film, include U.S. Pat. Nos. 3,872,483, issued to Numata et al, No. 3,882,512, issued to Lawrence et al, No. 3,968,505, issued to Kauneckas, No. 4,053,240, issued to Aizawa et al, No. 4,064,515, issued to Mashimo et al, No. 4,149,795, issued to Sakurda et al, No. 4,175,848, issued to Murakami et al, No. 4,361,388, issued to Micak et al, No. 4,635,203, issued to Merchant, No. 4,695,959, issued to Lees et al, No. 5,045,937, issued to Myrick, and No. 5,386,117, issued to Piety et al.

A secure communication system for static information is disclosed in U.S. Pat. No. 5,321,753, issued to Gritton. The message transmitted includes a 10-bit static first data field and a 54-bit second data field that changes from one transmission to the next. The 64-bit first and second data fields are encrypted and transmitted to a remote message reader that receives, decrypts and reads the transmitted message.

Goldfine et al disclose a financial or telephone service transaction authentication system, in U.S. Pat. No. 5,343,

529, in which any attempt to gain access to a protected system is thereafter answered and controlled by a centralized authentication agency. In response, the agency issues an identification request, requesting information that is unique to that request; a subsequent attempt by that person to gain access would require submission of different information. If the information supplied by the access seeker matches the information on file, the access seeker identity is authenticated and access is granted.

In U.S. Pat. No. 5,347,580, Molva et al disclose an authentication method using a smartcard to encrypt the presently displayed time with a cryptographically strong key. A public work station receives the encrypted time message, generates one or more values from this message, and further encrypts and/or transmits these values to a server station. The server station uses the received values to authenticate the holder of the smartcard and to accept or reject a message or command from the holder.

A remote control transmitter-receiver pair that cooperatively implement a code transmission sequence that minimizes energy use and protects the communication channel from unauthorized access is disclosed in U.S. Pat. No. 5,349,459, issued to Reed. The transmitter issues a specified sequence of start/stop pulses of different lengths, similar to pulse code modulation, which are received by the receiver and compared with a copy of this sequence. If the sequences agree, the receiver authenticates the transmitter and opens the secured channel to receive the remainder of the message.

Generation of each of two pseudorandom numbers, by an independently chosen number of iterations on initial numbers, is the basis for a cryptographic authentication system disclosed by Koopman et al in U.S. Pat. No. 5,363,448. The two pseudorandom numbers are concatenated and encrypted into a single word. This word is transmitted by or on behalf of a person seeking access to a protected system, and the word is decrypted and deconcatenated to produce the two pseudorandom numbers, for comparison and authentication purposes. Immediately after the concatenated and encrypted word is received, the receiving system locks out receipt of any additional signals for a selected time interval, such as 0.5 sec. Thus, breach of the protected system by rapid, exhaustive, numerical trials is made difficult or impossible.

Blume discloses a system to allow a space platform to distinguish between a friendly object and an unfriendly object in U.S. Pat. No. 5,382,957. The platform, which includes a GPS receiver/processor and antenna, transmits an encrypted interrogation signal to the object, which can be positioned tens or hundreds of kilometers from the platform, requesting certain information including the location coordinates of the object. Simultaneously, the platform uses high directivity radar and line of sight measurements to estimate the object range and the object location coordinates, using the platform's GPS-based knowledge of its own location. A friendly object will reply to the encrypted interrogation signal with an authenticating reply, including the GPS-determined location coordinates of the object. A receiver on the platform receives the object location coordinates from the object and compares these coordinates with its own estimate of the object location coordinates. If the object-supplied object location is within a determinable distance of the platform-supplied object location and all other authenticating replies from the object are appropriate, the platform authenticates the object as a "friendly" object.

In U.S. Pat. Nos. 5,384,846 and 5,388,158, Berson et al disclose methods for authentication of an identification card and the holder thereof. Several physical or other characteristics of the bona fide holder of the card are encrypted and recorded on a magnetic strip on the card, using a public key encryption scheme in which the key is changed from time to time. When the card is presented, the magnetic strip information is reproduced and compared with the corresponding characteristics of the card holder, to verify or refute the putative identity of the card holder. In another embodiment, the contents of a document are compressed, encrypted, encoded and placed on a two-dimensional bar code label for the document, for subsequent decryption and authentication of the document by reversing the process for the information on the label.

A GPS tracking system for a mobile station with physical sensors, relying upon receipt of unprocessed GPS signals that are initially received by the mobile station, is disclosed in U.S. Pat. No. 5,379,224, issued to Brown et al. Segments of the GPS signals received and time stamps are interleaved with sensor measurements of physical data and are transmitted to and processed by a central processing station, for estimation of the location of the mobile station at the time value given by the time stamp, and for examination of the physical sensor data. The GPS signals received from the mobile station are used for location determination, not for authentication of the asserted location of the central station.

Dent et al, in U.S. Pat. No. 5,390,245, disclose system for authentication of a base station and a mobile station that communicates with the base station. A first signal and a second signal are formed at each of the base station and the mobile station, and the base station transmits its first signal to the mobile station. The mobile station compares the received first signal with its own first signal to authenticate, or deny authentication to, the base station/transmitter. The mobile station then transmits its second signal to the base station for a similar authentication procedure by the base station.

A system for controlling the number of concurrently operating copies of a licensed software package is disclosed in U.S. Pat. No. 5,390,297, issued to Barber et al. Each node in a computer network is identified, for example, by number. If a given node requests use of, and contains a valid, unexpired license for, the software package, a license manager permits use of that software package at the given node. If an applicable license is not available at the given node, the license manager interrogates other nodes to find a license for the licensed software package that is not presently being used by that node and transfers the available license to the given node.

U.S. Pat. No. 5,406,619, issued to Akhteruzzaman et al, discloses a user authentication device for messages transmitted telephonically. The authenticator device, about the size of a credit card, is held against a telephone receiver and receives a query number as part of the telephone message. The authentication device uses its own key to transform the query number into an individualized response number that is transmitted as part of the same telephone cal to the query number initiator. Each of the query number and the response number is unique to the telephonic device used for that phone call.

A fire/security/control sensor access system that prevents unauthorized access by remote sensors is disclosed by Sanderford in U.S. Pat. No. 5,408,217. A central processor and a sensor unit communicate using one or more pseudo-random number sequences that is unique for that communicating pair, and each incoming and outgoing message must produce a "match" at the central processor and at the sensor before the transmitting sensor will accept reprogramming of its facility.

Evans discloses a sensor communication system with sensor polling in U.S. Pat. No. 5,440,301. Each remote sensor is polled for its present condition by a centrally located processor, using a unique coded signal that is received and analyzed by a receiver connected to the sensor. If the coded signal has a valid format, information stored in the receiver memory is transmitted in response to receipt of a polling signal.

In U.S. Pat. No. 5,442,342, issued to Kung, a distributed user authentication protocol is disclosed that prevents unauthorized access to any computer that is part of a network. Each network user is issued a coded card with a confidential message authentication code, which must be used to gain access to a computer on the network. The user must present the card and answer a sequence of randomly selected questions. At random times during use of a computer on the network, a user is required to again answer a randomly selected sequence of questions, in order to continue to use the computer.

Apparatus for controlling access to a device, such as an automated teller machine, at a secure location is disclosed by Heath in U.S. Pat. No. 5,451,757. A technician or other worker who seeks access to the device presents an access authentication message, including the worker's personal identification number (PIN), an access code presently stored at the device, and an access code of a portable computer terminal carried by the worker for use with the device. If the PIN and the two access codes are confirmed by the device, the worker is allowed access to the device. If access to the device is allowed, the access code presently stored at the device is immediately replaced by a new access code, to be used when requesting subsequent access to the device.

Steganography, which seeks to authenticate a graphical image by concealing a message in the image, is briefly discussed by S. Walton in "Image Authentication for a Slippery New Age," Dr. Dobb's Journal, April 1995, pp. 18–26. One method of concealment expresses each pixel in an electronic representation of the image in digital form and then alters the least significant bit of a chosen number of pixels to contain an authentication message.

These inventions usually rely upon some unchanging characteristic or combination of characteristics of an entity that seeks access to a protected system or a protected communication channel. The protection offered by these approaches might easily be compromised for a communication channel that is continually or periodically transmitting information. What is needed is an approach that relies in part on the constantly changing information associated with signals produced by a location determination system, to authenticate or verify the location and/or angular orientation of the entity that forms an image that is to be authenticated. Preferably, the information relied upon for, and specification of any pattern(s) used for, image authentication should be accurately and fully transmissible to another person or facility in confidence. Preferably, the approach should accept and work with confidential/encrypted signals and/or with signals that are available for use by any user with an appropriate receiver for a location determination system.

SUMMARY OF THE INVENTION

These needs are met by the invention, which forms a digitally expressed image, using a digital image formation means, such as a digital still camera or a digital video camera (referred to simply as a "digital camera"), and a digital image storage means, and conceals image authentication information concerning the circumstances of formation of the digital image of a selected view within the image itself. Preferably, this image authentication information includes location information and/or angular orientation information and/or information on time of image formation and/or distance from the digital camera to a selected object in a viewfinder for the camera (referred to collectively as "position information") of the digital camera at the time the digital image of the selected view is formed. This position information is provided, in part at least, by a location and/or angular orientation and/or time determination system, referred to as a position determination system ("PDS"), that is connected or attached to the digital camera and operates cooperatively with the digital camera. This position information is incorporated into the digitally expressed image or associated with the digital image.

If the position information is incorporated in the digital image, a chosen subset CS of pixels is selected, from the pixel array PA that forms an electronically or visually perceptible image in the digital camera, and the pixels in this chosen subset are individually altered to contain appropriate parts of the authentication information. This chosen subset CS of pixels for the image is determinable by, or known to, at least one person or facility so that this subset of pixels can be retrieved from the digital image and the authentication information can be recovered and analyzed. The pixels in this chosen subset CS may be contiguous or non-contiguous to each other and may be selected arbitrarily or according to some prescribed form, such as along a straight or curved line of pixels. Preferably, the pixels in the chosen subset CS are chosen so that any connected region of pixels in the pixel array PA with a pixel diameter greater than a selected threshold number will contain at least one pixel from the chosen subset CS.

Optionally, the locations of the chosen subset CS of pixels, or the particular bits within this chosen subset of pixels, whose pixel values are modified to contain the position information is specified by an authentication indicium, which may be a (large) single number or may be an ordered sequence of numbers. This authentication indicium, together with the digital image and associated position information may be transmitted as cleartext or may be encrypted and transmitted in encrypted form, to make it more difficult to alter the digital image or its asserted position information without detection.

Optionally, the position information and/or the specification of the chosen subset CS of pixels in which this information is concealed may be encrypted, using the location and/or orientation and/or time information (optional) provided by the PDS to determine the encryption key.

If the position information and/or the specification of the chosen subset CS is encrypted, a decryption technique, agreed upon in advance by those who are authorized to authenticate the image and position information, is applied to produce a readable message for that recipient. The encryption/decryption process may be a single key process, such as the Data Encryption Standard (DES) developed by IBM and disclosed in U.S. Pat. No. 3,798,360 and related patents, issued to Feistel. Alternatively, the encryption/decryption process may be a public key process, such as the recently developed RSA process, disclosed in U.S. Pat. No. 4,405,829 and related patents, issued to Rivest, Shamir and Adelman. The header and/or trailer of any satellite message would include one or more bits indicating: (1) whether this message is encrypted; (2) the beginning and end of the encrypted portion, if any, of this message; and/or (3) an identification by alphanumeric symbols of the key to be used by the recipient to decrypt any encrypted portion of this

message. When the selected recipient's receiver receives an encrypted message and an identification of the decryption key to be used, the receiver could automatically route this message to a decryption module that would read the key identification bits and apply the correct decryption key.

Optionally, the chosen subset of pixels may be partly or fully prescribed using the position information determined by the PDS at the time the digital image is formed by the digital camera.

This invention will be useful where a digital image and its associated authentication information is to be formed, preserved for later display and/or transmitted for use, analysis or display of the digital image by another user.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGS. 1 and 8 illustrate use of the invention in representative environments, where the location, angular orientation and/or time information for the PDS is provided by satellite sources of PDS signals and by ground-based sources of PDS signals, respectively.

FIG. 2 illustrates the angular coordinates used to determine angular orientation of a digital camera.

FIG. 3 is a schematic view of placement of three component antennas included in the antenna assembly for angular orientation determination according to one embodiment.

FIG. 4 illustrates determination of angular orientation by a means other than that used in FIG. 3.

FIG. 5 illustrates one suitable array of bits that provide location, angular orientation and/or time information according to the invention.

FIG. 6 illustrates several possible pixel patterns that can be chosen for storage of position information to be used for authentication of the digital image, according to one embodiment of the invention.

FIG. 7 is a schematic view of one embodiment of the digitized image forming apparatus and PDS signal antenna and receiver/processor apparatus according to the invention.

FIGS. 9A, 9B, 9C, 9D, 9E, 9F and 9G illustrate some suitable polygon coverings or overlays for the pixel array.

FIG. 10 illustrates use of a regular hexagon for image authentication pattern analysis.

FIG. 11 illustrates use of a non-equilateral hexagon for image authentication pattern analysis.

FIG. 12 illustrates use of an isoceles triangle for image authentication pattern analysis.

FIG. 13 illustrates use of a rectangle for image authentication pattern analysis.

FIG. 14 illustrates use of a parallelogram for image authentication pattern analysis.

DESCRIPTION OF BEST MODES OF THE INVENTION

FIG. 1 illustrates use of the invention in one environment. A user 11, positioned at a particular location with location vector $r_u=(x_u, y_u, z_u)$ in a selected coordinate system, points or orients a digitized image forming device ("digital camera") 13 in a selected direction having an orientation vector $r_o=(\cos\phi \sin\theta, \sin\phi \sin\theta, \cos\theta)$, where ϕ is the azimuthal angle and θ is the polar angle of the vector r_o, measured relative to the axes of the selected coordinate system, as indicated in FIG. 2. In FIG. 2, for definiteness, the coordinate system used for (x_u, y_u, z_u) is assumed to be a three-dimensional Cartesian system. However, the coordinate system CS can also be a three-dimensional or two-dimensional coordinate system, as noted above.

A position determining system ("PDS") signal antenna assembly 15 in FIG. 1 is rigidly attached to the digital camera 13 and receives a PDS signal from each of a plurality of PDS satellite sources 19A, 19B, 19C, 19D, etc. of the PDS signals and passes the PDS signals to a PDS signal receiver/processor 17 that is preferably also attached to the digital camera 13. Alternatively, the PDS receiver/processor 17 can spaced apart from, be linked to and receive signals from the PDS antenna assembly 15 by a cable link or a wireless link 21L (optional). Optionally, the digital camera 13 includes a rangefinder 16 that determines and records the distance d from the camera lens or other digital image-forming mechanism to a selected object O in the selected view.

The PDS receiver/processor 17 receives the PDS signals from the PDS antenna assembly 15 and determines the location and/or angular orientation of the PDS antenna assembly (or digital camera) and/or time of receipt/observation of the PDS signals, using the times of arrival of the PDS signals from the different PDS satellite signal sources 19A, 19B, 19C, 19D and the known locations of these sources at any given time. The PDS satellite signal sources may belong to a Global Positioning System ("GPS"), to a Global Orbiting Navigational Satellite System ("GLONASS") or to any other suitable geosynchronous or non-geosynchronous satellite system that broadcasts timed signals that can be used to determine location and/or angular orientation and/or time of receipt/observation of a receiver of such signals, such as the Motorola 66-satellite Iridium system or the LEO (Low Earth Orbit) satellite system.

If angular orientation (ϕ,θ) of the digital camera 13 is to be determined, the PDS signal antenna assembly 15 includes three or more spaced apart, non-collinear, PDS signal-receiving component antennas 15-1, 15-2, 15-3, shown in FIG. 3, that define a plane or other two-dimensional surface and whose distances from each other are known and preferably fixed. In this configuration, a PDS signal received at each of the component antennas 15-1, 15-2, 15-3 from a given satellite source, such as 19B, is received by multiplexing at the PDS receiver/processor 17; and the different times of arrival of this PDS signal at the different component antennas determines the angular orientation of a plane or other geometric object containing these component antennas. The PDS component antennas 15-1, 15-2, 15-3 may be rigidly attached to the digital camera 13. Alternatively, one or more of these PDS component antennas 15-2 and/or 15-3 may be snappable into place at fixed angles and at fixed distances relative to another component antenna 15-1, whose location on the digital camera 13 is fixed.

Alternatively, where angular orientation (ϕ,θ) of the digital camera 13 is to be determined, this orientation information can be determined using attitude-sensing means other than the three or more location-sensing antennas shown in FIG. 3. Angular orientation or attitude of the digital camera 13 can be sensed by using two or more accelerometers, by using two or more gyroscopes, or by using two or more magnetic field-sensing instruments, referenced to the local direction and/or magnitude of the Earth's magnetic field, as indicated schematically in FIG. 4. Any other accurate attitude or angular orientation sensor 18 that does not rely upon PDS-based determination of the location of a plurality of PDS signal antennas can also be used to determine angular orientation of the digital camera 13.

If angular orientation (ϕ,θ) of the digital camera 13 need not be determined, the PDS signal antenna assembly 15 may include a single antenna, to be used to receive PDS signals at a location that is rigidly attached to the digital camera.

The user **11** points or orients the digital camera **13** and records a digital image of a selected view, as indicated in FIG. **1**. At the time this image is recorded, the PDS antenna assembly **15** and PDS receiver/processor **17** receive and analyze PDS signals and determine the present location and/or angular orientation and/or time of receipt/observation of the PDS signals, referred to collectively as "position information" for convenient reference. Optionally, this position information includes the camera-object distance d determined by the rangefinder **16**, discussed above.

In a first embodiment of the invention, the position information is automatically recorded separately at the time the digital image of the selected view is recorded, and the digital image and the position information are associated or bound together for future use. For example, the digital image may be recorded in sub-frame N-1 and the position information may be recorded in a contiguous sub-frame N-2 (of smaller size), which are both parts of frame N. Sub-frame N-2 is illustrated in FIG. **5** as a linear bit array BA of bits, including an optional header having H1 bits, B1 bits containing the location coordinates or related location information for the digital camera, B2 bits containing the angular orientation coordinates or related orientation information for the digital camera, B3 bits containing time of receipt/observation information for the digital camera, and an optional trailer containing H2 bits. The numbers H1, B1, B2, B3 and H1 are non-negative integers, and least one of the integers B1, B2 and B3 is positive.

In FIG. **5**, B1 or B2 or B3 is a positive integer only if the corresponding position information item (location, orientation or time) is recorded and included in the bit array BA. If location information is recorded, for example, each of the two or three location coordinates x_u, y_u and/or z_u might be allocated 16 or more bits in the bit array BA to express the corresponding location coordinate in the location coordinate system chosen (Cartesian, polar, cylindrical, spherical, ellipsoidal, etc.) for such representation. If angular orientation information is recorded, each of the one or two angular coordinates ϕ and/or θ might be allocated 16 or more bits in the bit array BA. If time information is recorded, this information might be allocated 16 or more bits in the bit array BA.

In a second embodiment of the invention, the position information is recorded as a visually perceptible overlay on the digital image of the selected view formed by the digital camera **13**. This overlay preferably includes the location information and/or the angular orientation information and/or the time information for the PDS signal antenna assembly **15** at the time the digital image is formed. This overlay, illustrated in FIG. **6** as a region designated as "position information," is preferably located near a boundary or other selected site on the digital image that is unlikely to interfere with visual perception of the important details in the digital image of the selected view. This embodiment offers the advantage that the position information is viewable when the digital image is viewed.

In a third embodiment of the invention, the position information is automatically recorded or embedded as part of the corresponding digitally expressed image formed by the digital camera, using a pixel array PA such as shown in FIG. **6**. An authentication pattern P of pixels, which is a chosen subset CS of pixels in the array PA of all pixels representing the digital image, is selected. For each pixel in the pattern P, one or more bits in the representation of the pixel value is replaced by a bit in the bit array BA, and the original digital image is re-formed as a modified digital image, now containing the position information recorded at the time the original digital image was formed. It is the modified digital image that is stored in the digital camera. The pixel value corresponding to the original digital image may be: (1) a binary value (one bit, black or white, used for text and for line drawings and line graphical images); (2) a gray scale value (J bits with $J \geq 2$, used to represent gray scale images with black, white and up to 2^J-2 gray scales lying between black and white); (3) color values (J bits with $J \geq 8$, used to represent R,G,B or C,Y,M,K or some other suitable expression of up to 2^J colors in a spectrum, including black and white); and (4) any other suitable pixel value representation.

FIG. **6** illustrates several possible authentications patterns P that may be chosen here but is not intended to exhaust the possibilities. Possible patterns include a linear contiguous pattern P1 of pixels, a curvilinear contiguous pattern P2 of pixels, a pattern P3 of non-contiguous pixels located on a line, a geometric pattern P4 of non-contiguous pixels located on a curve, a geometric pattern P5 of non-contiguous pixels located along an open or closed linear or curvilinear polygon, and a randomly selected pattern P6 of pixels.

The authentication pattern P6 may be selected by reference to, or using, the position information recorded with the digital image. As one example of this selection, if the pixels in the digital representation form an M×N array, assign a distinct number m=0, 1, 2, . . . , M×N−1 to each pixel in the pixel array PA. Now express the recorded position information, not as a bit array a shown in FIG. **5**, but as a more familiar decimal array of "decimal integers" (each being 0, 1, 2, 3, 4, 5, 6, 7, 8 or 9, a decimal point, or a sign bit ±1). In this decimal array, each of the location coordinates x_u, y_u and/or Z_u is allocated Q+1 decimal integers, each of the angular coordinates ϕ and/or θ is allocated R decimal integers, and the time information is allocated S decimal integers, where Q, R and S are non-negative integers. Assume that the location coordinates x_u, y_u and z_u are expressed as $(\epsilon_x, d_{x,1}, d_{x,2}, \ldots, d_{x,Q})$, $(\epsilon_y, d_{y,1}, d_{y,2}, \ldots, d_{y,Q})$ and $(\epsilon_z, d_{z,1}, d_{z,2}, \ldots, d_{z,Q})$, respectively, where ϵ_x has the value +1 or −1, corresponding to the sign of the coordinate x_u, and each of the quantities $d_{x,n}$ (n=1, 2, . . . , Q) is a decimal integer. The pixel pattern P is then chosen as follows. Beginning with the pixel numbered m=m0=0, if ϵ_x=+1, or with the pixel numbered m=m0=1, if ϵ_x=−1, in the pixel array PA, the first Q pixels in the pattern P correspond to the pixel array numbers m0+2$d_{x,1}$, m0+2$d_{x,1}$+2$d_{x,2}$, . . . , m0+2$d_{x,1}$+2$d_{x,2}$+ . . . +2$d_{x,Q}$=m0'. This encodes the location coordinates x_u. Beginning with the pixel numbered m1=m0', if ϵ_y=+1, and with the pixel numbered m1=m0'+1, if ϵ_y=−1, the next Q pixels in the pattern P correspond to the pixel array numbers m1+2$d_{y,1}$, m1+2$d_{y,1}$+2$d_{y,2}$, . . . , m1+2$d_{y,1}$+2$d_{y,2}$+ . . . +2$d_{y,Q}$=m1'. This encodes the location coordinates y_u. This selection of pixel locations continues with the Q pixel locations corresponding to the location coordinate z_u, the R pixel locations corresponding to the angular coordinate ϕ, the R pixel locations corresponding to the angular coordinate θ, and the S pixel locations corresponding to the time information.

The set of pixel locations in the authentication pattern P is a maximum of 3Q+2R+S pixels, although fewer pixel locations can be used if desired. This set of (at most) 3Q+2R+S pixel locations can be augmented by additional pixel locations selected using information in addition to the position information. Alternatively, the set of pixel locations in the pattern P used to record the position information can be generated according to some other selection procedure, including purely random pixel selection.

The authentication pattern P should be chosen so that every region π of pixels in the array PA with diameter

(measured in units of pixel-to-pixel nearest neighbor distance) satisfying dia(π)≧D has at least one pixel from the pattern P in the region π, where D is a selected value, for example, in the range 5–100. The value D is chosen so that any visually perceptible object of a size at least, say, 0.1–1 cm, when measured on the pixel representation of the digital image, will have at least one pixel from the pattern P. This requires that the density of pixels belonging to the chosen subset CS, within the pixel array PA, be at least equal to a threshold value. One approach for implementing this density requirement is to require that, for any given pixel in the array PA, a circle of diameter D and centered at the given pixel contains at least one pixel in the chosen subset CS.

Alternatively, the pattern P can be a large fraction, such as 50–100 percent, of all the pixels in the array PA, in an interleaved pixel pattern, so that it is substantially impossible to alter the pixel value of two or more contiguous pixels in the digital image without discovery. However, this would require use of a relatively slow procedure to form the modified digital image and use of a relatively slow procedure to analyze and authenticate a putative image of the selected view.

Once the authentication pattern P is selected, one or more bits in the pixel value representation for each pixel in the pattern P is replaced by a bit from the ordered bit array BA (FIG. 5) that represents the position information. In one preferred mode of this second embodiment, the least significant bit ("LSB") of each of the pixel value representations for pixels in the pattern P is replaced by a bit in the bit array BA. Where gray scale or color representations of an image are used with N≧8 bits, change of the LSB from 0 to 1, or from 1 to 0, will not be detectable by most persons so that after such LSB replacement the modified digital image (in visually perceptible form) will be substantially the same as the original digital image.

In a second mode of this third embodiment, two or more bits, or even all bits, in a pixel value representation, for one or more pixels in the authentication pattern P, are replaced by bits from the bit array BA (FIG. 5) of position information. With this last mode implemented, the modified visually perceptible image may be substantially different from the original visually perceptible image and may have a "salt and pepper" visual appearance wherever the number of pixels in the pattern P in a region of the pixel array PA is large.

In the first, second or third embodiment, the position information, shown in bit array format in FIG. 5, can be presented in cleartext or can be encrypted, using an encryption algorithm with a selected encryption key and a corresponding decryption key. The selected encryption key can be prescribed independently of the content of the position information.

Alternatively, the encryption key can depend upon the content of the position information. In this alternative approach, a selected part of, or all of, the position information is treated as one or more parameters that determine the encryption key. For example, the location information and/or angular orientation information and/or time information can be expressed in bit array format and can be combined, bit by bit, with a selected bit pattern of appropriate length L, using EXclusive Or or EXclusive NOR or twos complement addition, to form an encrypted bit array BA_{enc}. The encrypted bit array BA_{enc} is then placed in the second sub-frame associated with the digital image in the first sub-frame (first embodiment) or is used to replace selected bits in the pixel value representation for the pixels in a pixel pattern P, such as shown in FIG. 6.

FIG. 7 schematically illustrates one embodiment of PDS/digital camera apparatus 31 according to the invention. A digitally expressed image of an object O is captured by means of a digital camera lens, focusing and shutter mechanism 33 and is passed through a PDS/camera interface 35. The PDS/camera interface 35 also receives information from a PDS signal receiver/processor 17 that determines position information (location coordinates and/or angular orientation coordinates and/or time of observation of position and/or distance to the object O) based upon PDS signals received at a PDS signal antenna assembly 15. Optionally, the PDS signal antenna assembly 15 may include a single PDS signal antenna 15-1 or may include two or more PDS signal component antennas 15-1, 15-2, 15-3. Optionally, a rangefinder 37, with an optical or electronic signal that can be directed to a selected object O in the selected view, that provides information on the distance d from the digital camera lens mechanism 33 to the object O for analysis and/or digitization by the PDS receiver/processor 17.

Optionally, the apparatus 31 includes an attitude or angular orientation sensor 18 that uses signals that are partly or fully independent of the PDS signals received at any of the PDS antennas 15-1, 15-2, 15-3, such as accelerometer signals, gyroscopic signals or magnetic field signals from the Earth's local field, to determine the angular orientation or attitude of the apparatus 31 at the time a digital image is formed. In this instance, use of a single PDS antenna 15-1 may suffice here.

The PDS/camera interface converts the image of the object O captured by the lens mechanism 33 into an array of K-bit, digitally expressed pixel values, using a CCD (charge coupled device) array or other array of M×N optical sensors, with each pixel or cell corresponding to a pixel or picture element for the digital image. The number of bits K for each pixel value may be K≧1 for text or simple line drawings, K≧8 for gray scale images, and K≧16 (preferably K≧32) for color images. Where a color image is captured and digitally expressed by the lens mechanism 33, 8 bits may be used for expressing image intensity and K-8 bits may be used to express the color hue and/or color saturation data for the image. The pixel array size may be M×N=100×133, 480×640, 480×720, or some smaller or larger size.

The digitally expressed image for the object O is combined or paired with the digitally expressed position information received from the PDS receiver/processor 17 at the PDS/camera interface 35 and is passed through an encryption module 38 (optional) to a digital frame recording and storage module 39 for "permanent" storage therein as a digital frame or file. As noted above, the digital image and the corresponding digitized position information may be stored as two subframes that are part of the same digital frame, or the position information may be stored as part of the digital image, with one or more altered pixel value bits that contain position information. Optionally, a sequence of two or more digital frames, such as a digital video sequence, may be thus formed, recorded and stored in the frame recording and storage module 39. A digital frame is optionally assigned a corresponding index number, unique for each frame, and this index number is stored in an indexing module 41 with an adjustable pointer that indicates which digital frame in the frame recording and storage module 39 corresponds to this index number. Optionally, the indexing module 41 allows specification of which portion of the digital frame is to be displayed (or downloaded through a download port 45, discussed below) and the format to be used for such display.

If information on one or more digital frames stored in the frame recording and storage module 39 is to be visually or

audibly displayed (optional), the index number(s) corresponding to the digital frame(s) is specified at the indexing module 41. A copy of a specified digital frame, or portion thereof, is sent to a digital frame display or playback module 43, for viewing of the digitally expressed image(s) of the object O and/or of the corresponding position information in graphical or alphanumeric format. The format for display of the position information contained in a digital frame may be in terms of latitude, longitude, elevation, orientation angle (s), observation time and/or lens-to-object distance. Alternatively, the location coordinate information contained in a digital frame may be expressed in terms of local coordinates or in terms of another global coordinate system. Optionally, a visually perceptible map with an adjustable scale, drawn from a collection of maps stored in a map storage module 45, may be provided at the digital frame display module 43 that graphically indicates by an icon the location of the apparatus 31 at the time a specified digital frame was formed.

Part or all of the information contained in a digital frame stored in the frame recording and storage module 39 may be downloaded, using a digital frame information download port 47, and/or transmitted, using an optional transmitter and antenna 50, that are connected to the module 39. Downloading or transmission of this information is, optionally, performed by an authorized digital frame downloader who uses an optional special software key (e.g., a confidential or encryption key) or an optional special hardware key to request and implement the frame information download.

The digital image and the associated position information are downloaded directly from the digital frame recording and storage module 39, possibly using a portion of or all of the position information to provide a key for decryption and/or to provide a key for determining the pattern P of pixels used to hold the position information. Authentication of the image is provided by comparing the position information contained in the digital frame with the putative position information that is asserted or is on file elsewhere. If the downloaded or displayed position information and the putative position information substantially agree, the corresponding digital image on that frame may be authenticated. If the downloaded or displayed position information and the putative position information do not substantially agree, authentication of the corresponding digital image on that frame may be withheld.

The digital camera 33 may use an array of charge coupled devices ("CCDs"), magnetic tape recording or other suitable devices and media to record the digital images. Various approaches for digital recording of an image in a digital still camera br a digital video camera are discussed in U.S. Pat. Nos. 4,074,324, issued to Barrett, No. 4,131,919, issued to Lloyd et al, No. 4,489,351, issued to de Costemore d'Arc, No. 4,541,010, issued to Alston, No. 4,626,898, issued to Baba et al, No. 4,680,628, issued to Wojcik et al, No. 4,702,585, issued to Harada et al, No. 4,704,632, issued to Van Den Heuvel, and No. 4,837,628, issued to Sasaki. The information in these patents is incorporated by reference herein.

One method of recording the digital frame uses a three-state, Read Only Memory (ROM) chip. The ROM chip has a plurality of activatable sites, each with an initial, pristine state and distinct, first and second activated or burned-in states. When a digital image is formed by the digital camera, the initial, pristine state at each site is converted into a first activated state or into a second activated state, after which no further state change is possible. Alternatively, a two-state ROM chip may be used here.

The digital frame thus formed may, optionally, be protected by locking down the frame so that the frame can be visually or audibly perceived using the digital frame display 43 but cannot be downloaded except by use of a confidential key that is held by a certified digital image downloader. Alternatively, this confidential key may be decomposed into two or more key components, and each component may be held by a separate certified digital frame downloader.

Alternatively, the PDS signal antenna assembly 15 and PDS signal receiver/processor 17 can receive PDS signals from ground-based PDS signal sources, such as signal towers or other substantially stationary sources 29A, 29B, 29C, 29D in a Loran-C, Tacan, Decca, Omega or Metricom system, as illustrated in FIG. 8.

Assume that the pixels in the pixel array PA are numbered n=1, 2, . . . , N and that the pixels in the chosen subset CS used for image authentication correspond to n=n1, n2, n3, . . . , nA, where A is a positive integer less than N. List the set PN of prime numbers (not divisible by any integer greater than 1 that is less than the number itself) in increasing order as p(1)=2, p(2)=3, p(3)=5, p(4)=7, p(5)=11, etc. up to n=N. For example, p(25)=97 and p(168)=997. According to a theorem of Euler the number of prime numbers is infinite so that for any integer N one can, in principle, find the prime number p(N). The number of prime numbers no greater than M is known to be approximately equal to $M/\log_{10}(M)$ so that the Nth prime number p(N) increases quickly with the integer N.

Now define a sequence of numbers

$$q(m) = 1 \quad \text{if pixel } m \text{ does not belong to } CS \qquad (1)$$
$$= p(m) \quad \text{if pixel } m \text{ belongs to } CS,$$

and define an authentication indicium Q by

$$Q = \prod_{m=1}^{N} q(m). \qquad (2)$$

The number Q has A prime number divisors, corresponding to the A numbers n=n1, n2, . . . , nA in the chosen subset CS, and for any chosen subset CS of A pixels ($1 \leqq A < N$) a corresponding number Q, defined by Eq. (1), can be found. The correspondence between Q and the particular pixels in the chosen subset CS is thus one-to-one. The set of pixel locations in the chosen subset CS is thus prescribed uniquely by the single number Q. Thus, one can transmit a frame, consisting of the image to be authenticated and position information for the digital image formation means plus the number Q and thereby fully specify the image and its authentication pixel pattern CS. The set PN of prime numbers can be replaced by any other countable, infinite set S of distinct numbers (real or complex) $\{z_n\}_n$ for which, given any (real or complex) number z in a selected group, a unique factorization of z into multiplicative factors drawn from S exists.

Note that the authentication indicium Q in this approach does not contain the position information itself; Q merely determines the locations in the pixel array PA at which the pixel bit values have been modified to contain the position information. Specification of the indicium Q allows a user to (1) identify the locations of the chosen subset CS of pixels in the pixel array PA at which the pixel bit values have been modified to contain the position information, (2) retrieve the pixel values for the chosen subset CS of pixels, and (3) retrieve the position information contained in the modified pixel bit values in the chosen subset CS of pixels.

If each pixel in the pixel array PA has an associated pixel value that is expressed as an ordered set of K pixel bits (K=1,

8, 16 or 24, for example), this first approach can be extended by first numbering all pixel bits m=1, 2, . . . , K-N, where K is the number of bits in a pixel value. Define CS' to be the set of integers, drawn from the set {1, 2, . . . K-N}, corresponding to pixel bits that are modified to contain the position information. Now define

$$q'(m) = 1 \quad \text{if bit } m \text{ does not belong to } CS' \qquad (3)$$
$$= p(m) \quad \text{if bit } m \text{ belongs to } CS'.$$

Finally, define an authentication indicium Q' by the product

$$Q' = \prod_{m=1}^{K\cdot N} q'(m). \qquad (4)$$

The authentication indicium Q' plays the same role in this second approach that the indicium Q plays in the first approach, except that Q' now identifies the particular pixel bits whose values are modified to contain the position information.

In a third approach, an indicium can be defined using sums rather than products of numbers. Define another sequence of numbers

$$r(m) = 0 \quad \text{if pixel } m \text{ does not belong to } CS \qquad (5)$$
$$= 1 \quad \text{if pixel } m \text{ belongs to } CS,$$

and define an authentication indicium R by

$$R = \sum_{m=1}^{N} r(m)2^{-m}. \qquad (6)$$

The maximum value of R is $1-2^{-N}$ ($\leqq 1$), and each pixel that is a member of the chosen subset CS makes a unique, measurable contribution to the indicium R. More specifically, the indicium R in Eq. (6) may be re-expressed in binary form as (r(1), r(2), r(3), . . . , r(N)), where a coefficient r(m)=1 if and only if pixel m belongs to the chosen subset CS. Any number of the form $w/2^N$ (w=0, 1, 2, 3, . . . , 2^N-1) can be re-expressed in the form of Eq. (6) and thus corresponds to a particular choice of pixel locations in the chosen subset CS.

More generally, for any choice of a real number Z>1 an authentication indicium

$$R(Z) = \sum_{m=1}^{K\cdot N} r(m)Z^{-m} \qquad (7)$$

can be defined in which each pixel that is a member of the chosen subset CS makes a unique, measurable contribution to the indicium R(Z). By analogy with the re-expression of Eq. (6) in binary form, Eq. (7) can be re-expressed in Z-ary form as (r(1), r(2), r(3), . . . , r(N)), in which the kth element r(k) (k=1, . . . , N) in this sequence has an associated weight of Z^{-k}. The maximum value of the indicium R(Z) is $\{1-Z^{-N}\}/(Z-1)$.

By analogy with the development of Eqs. (3) and (4), if each pixel in the pixel array PA has an associated pixel value that is expressed as an ordered set of M pixel bits (M=8, 16 or 24, for example), this first approach can be extended by first numbering all pixel bits n=1, 2, . . . , K-N.

Define CS' to be the set of integers, drawn from the set {1, 2, . . . K-N}, corresponding to pixel bits that are modified to contain the position information. In a fourth approach, define

$$r'(m) = 0 \quad \text{if bit } m \text{ does not belong to } CS \qquad (8)$$
$$= 1 \quad \text{if bit } m \text{ belongs to } CS',$$

and define an authentication indicium R' by the product

$$R'(Z) = \sum_{m=1}^{K\cdot N} r'(m)Z^{-m} \qquad (9)$$

The authentication indicium R'(Z) plays the same role in this fourth approach that the indicium or R(Z) plays in the third approach, except that R'(Z) now identifies the particular pixel bits whose values are modified to contain the position information.

If the number K-N of pixels in the pixel array PA is large, the number Q or Q', as defined in Eq. (2) or (4) will be very large; and the number of Z-ary digits required for the Z-ary expression (r(1), r(2), r(3), . . . , r(N)) or (r(1), r(2), r(3), . . . r(K-N)) will also be very large. One method of reducing a number such as Q or Q' or N or K-N to manageable size is to decompose the pixel array PA into a plurality of smaller, preferably non-overlapping sub-regions of similar or identical shape and size and to apply the analysis indicated in Eqs. (1) and (2), in Eqs. (3) and (4), in Eqs. (5) and (6), or in Eqs. (8) and (9), to each sub-region separately. This approach is also useful in limiting, if not eliminating, the amount of image alteration that can go undetected.

The pixel array PA can be tesselated by a numbered set of convex, regular, identical polygons (all sides having the same length, with vertices lying on a single circle) that cover the pixel array PA, using equilateral triangles, squares or regular hexagons. To this list of convex, regular polygons one can add isosceles triangles, rectangles, parallelograms and non-equilateral hexagons (having sides with the same length but not having identical interior angles) to obtain a numbered set TP of two-dimensional tesselation polygons, to each of which the analysis indicated in Eqs. (1) and (2), in Eqs. (3) and (4), in Eqs. (5) and (6), or in Eqs. (8) and (9) is applied, covering the pixel array PA, as a polygon overlay in which each pixel lies in precisely one polygon of the overlay. These seven classes of polygons are illustrated in FIGS. 9A, 9B, 9C, 9D, 9E, 9F and 9G, respectively.

For purposes of illustration, consider a tesselation of a pixel array PA by a numbered assembly TP of convex, regular hexagons h_g (g=1, 2, . . . , G), as indicated in FIG. 9C. A hexagon that is located near an edge of the pixel array PA may contain fewer pixel locations than a hexagon that is located in the interior of the pixel array PA, but the analysis is the same.

A representative regular hexagon h, shown in FIG. 10, has a top-to-bottom width of λ_y, a vertex-to-vertex length of $\lambda_x=(2/\sqrt{3})\,\lambda_y$ ($>\lambda_y$), and an area of $(\sqrt{3}/2)(\lambda_y)^2$, with the hexagon orientation shown in FIG. 10. For example, if $\lambda_y=6$, $\lambda_x=4\sqrt{3}=6.928$, and the corresponding hexagon area is $A_{hex}=31.177$. For this particular hexagon, six horizontal pixel lines, spaced 1.0 units apart, with each horizontal line containing pixels at intervals of 1.0 unit as shown, are set down within the hexagon at line "heights" of $\Delta y=\pm 0.5$ units, ± 1.5 units and ± 2.5 units relative to the center C of the hexagon. The hexagon h contains an average m_{hex} of 31–32 pixel locations, the maximum distance d_{hex} from the center C to a pixel location within h is

$$d_{hex}=\sqrt{8.5}=2.915, \qquad (10)$$

and the diameter D_{hex} of this hexagon is

$$D_{hex}=\lambda_x=6.928. \qquad (11)$$

More generally, for a regular hexagon of width λ_y and length $\lambda_x=(2/\sqrt{3})\,\lambda_y$, and a general choice of locations of

horizontal lines spaced 1.0 units apart, the maximum distance of a pixel from the center C, the hexagon diameter and the hexagon area are given by

$$d_{hex} \leqq \lambda_y/\sqrt{3}, \tag{12}$$

$$D_{hex}=2\,\lambda_y/\sqrt{3}, \tag{13}$$

$$A_{hex}=6\,(\lambda_x/4)\,(\lambda_y/2)=\sqrt{3}\,(\lambda_y)^2. \tag{14}$$

The distances d_{hex} and D_{hex} and area A_{hex} scale linearly, linearly and quadratically, respectively, with the choice of λ_y. The number m_{hex} of pixel locations within the hexagon h scales monotonically but nonlinearly with the choice of λ_y.

Preferably, the pixel locations in the array PA are uniformly spaced apart and the hexagons are positioned so that each pixel location is in one hexagon and is not located on a boundary of any hexagon. The pixel locations within a hexagon h_g (numbered g=1, 2, . . . , G) are numbered m=1, 2, . . . , m_{hex}. At least one pixel in the chosen set CS is selected in each hexagon h_g, and the distance D of any pixel within such a hexagon from a pixel in the chosen set CS within that hexagon is easily verified to be

$$D \leqq 2\,d_{hex}=5.831, \tag{15}$$

for the choices $\lambda_x=4\sqrt{3}$ and $\lambda_y=6$. As noted, the distance D is proportional to the distance d_{hex} and thus scales linearly with λ_y. If, for example, it is desired that the maximum distance of any pixel from the nearest pixel in the chosen set CS satisfy D≦5 (in units of pixel-to-pixel nearest neighbor distance), a new array of identical hexagons is selected. The vertex-to-vertex length λ_x and the top-to-bottom width λ_y are chosen as

$$\lambda_y \leqq (5/5.831)\,6=5.164, \tag{16}$$

$$\lambda_x=(2/\sqrt{3})\,\lambda_y=5.962. \tag{17}$$

for each new hexagon in the new array. This new array satisfies D≦5.

The hexagons in the array are assigned numbers h_g with g=1, 2, . . . , G, and each pixel within the hexagon h_g is assigned a number m=1, 2, . . . $m_{hex,g}$, where $m_{hex,g}$ is the number, discussed above, of pixels within the hexagon h_g. The number $m_{hex,g}$ may be constant or may vary slightly from one hexagon to the next, depending on the size, location and orientation of each hexagon relative to the pixel array PA. Within each hexagon h_g, a sub-indicium $I_g=Q_g$ or $I_g=Q'_g$ or $I_g=R(Z)_g$ or $I_g=R'(Z)_g$ (written as "I_g" for convenient reference) for members of the chosen subset CS that are within the hexagon h_g (denoted "CS_g") is calculated, and the hexagon h_g is assigned the indicium component (g, I_g). For example, if the selected sub-indicium is $I_g=Q_g$ or $I_g=R(Z)_g$, I_g is calculated using the respective definitions

$$q(m)_g = 1 \quad \text{if pixel } m \text{ does not belong to } CS_g \tag{18}$$
$$= p(m) \quad \text{if pixel } m \text{ belongs to } CS_g,$$

$$Q_g=\prod_{m=1}^{N} q(m)_g, \tag{19}$$

$$r(m)_g = 0 \quad \text{if pixel } m \text{ does not belong to } CS_g \tag{20}$$
$$= 1 \quad \text{if pixel } m \text{ belongs to } CS_g,$$

-continued

$$R(Z)=\sum_{m=1}^{N} r(m)_g Z^{-m}. \tag{21}$$

The position of each hexagon h_g is assumed to be known, relative to the pixel array PA. The pixel array PA is then assigned an authentication indicium I, such as

$$I=(1,I_1;\ 2,\ I_2;\ \ldots\ ;\ G,\ I_G), \tag{22}$$

which characterizes the chosen subset CS for the regular hexagon array shown in FIG. 9C.

A hexagon hex_g, shown in FIG. 11, from the array of non-equilateral hexagons in FIG. 9G with fixed interior angles φ1 (<120°) and φ2 (>120°), is similarly analyzed, and the corresponding vertex-to-vertex length λ'_x and top-to-bottom width λ'_y are determined. If each side of the hexagon hex_g has length s, the parameters λ'_x and λ'_y are determined by the relations

$$\lambda'_x=s\,(1-2\,\cos\phi 2), \tag{23}$$

$$\lambda'_y=2s\,\cos(\phi/2), \tag{24}$$

where the interior angles φ1 and φ2 are fixed. The corresponding maximum distance $d'_{hex,g}$ from the hexagon center C to any pixel location within the hexagon hex_g, the diameter $D'_{hex,g}$ of the hexagon hex_g, and the area $A_{hex,g}$ of the hexagon hex_g scale linearly, linearly and quadratically, respectively, with the choice of value for the parameter λ'_x or λ'_y or s for that hexagon. The number $m'_{hex,g}$ of pixel locations in the array PA that lie within the hexagon hex_g will increase monotonically but nonlinearly with the parameter λ'_x or λ'_y or s for that hexagon. The collection of hexagons hex_g that cover the array PA of pixels is then numbered g=1, 2, . . . , G, a sub-indicium I_g is then calculated for each hexagon hexg as discussed above, and the pixel array PA is assigned an authentication indicium

$$I=(1,I_1;\ 2,\ I_2;\ \ldots\ ;\ G,\ I_G) \tag{25}$$

characterizing the chosen subset CS.

Proceeding by analogy, an isoceles (or equilateral) triangle tr_g with interior angles φ1, φ1 and φ2 (which may all be=60°) and base length b (in units of nearest neighbor pixel-to-pixel distance), shown in FIG. 12, has a center C and has a length λ_x=b and a width λ_y=0.5 b tanφ1 in the x-direction and in the y-direction, respectively. For any set of horizontal lines containing pixel locations imposed on the triangle tr_g, the maximum distance $d_{tr,g}$ from the center C to any pixel location within this triangle is the distance of the center C to any vertex and is given by

$$d_{tr,g}=0.25\,b\,\sec\phi 1\,\csc\phi 1. \tag{26}$$

Assume that each triangle, such as tr_g, in the array shown in FIG. 9A or 9D contains at least one pixel from the chosen subset CS. The maximum distance $D_{tr,g}$ from any pixel location in the triangle tr_g, to a pixel location in the chosen subset CS within tr_g is then bounded by

$$D_{tr,g} \leqq 2\,d_{tr,g}=0.5\,b\,\sec\phi 1\,\csc\phi 1, \tag{27}$$

and this upper bound on the distance $D_{tr,g}$ can be raised or lowered by varying the base length b. The pixel locations

within the triangle tr_g are consecutively numbered m=1, 2, . . . , $m_{tr,g}$, and the sub-indicium I_g is calculated for each triangle tr_g. An authentication indicium

$$I=(1, I_1; 2, I_2; \ldots; G, I_G) \quad (28)$$

is associated with the array of triangles tr_g for the pixel array PA, characterizing the chosen subset CS.

Proceeding by analogy, a rectangle (which may be a square) rec_g has length λ_x and width λ_y in the x-direction and in the y-direction, respectively, where the ratio $r=\lambda_y/\lambda_x$ is assumed to be fixed, is shown in FIG. 13. The maximum distance from the rectangle center C to any pixel location within the rectangle rec_g is given by

$$d_{rec,g}=0.5\,[1+r^2]^{1/2}\lambda_x \quad (29)$$

and the maximum distance $D_{rec,g}$ from any pixel location in the rectangle rec_g to a pixel location in the chosen subset CS within rec_g is then bounded by

$$D_{rec,g}\leq 2\,d_{rec,g}=[1+r^2]^{1/2}\lambda_x \quad (30)$$

This upper bound can be raised or lowered by varying the length λ_x. The pixel locations within the rectangle rec_g are consecutively numbered m=1, 2, . . . , $m_{rec,g}$, and the sub-indicium I_g is calculated for each rectangle rec_g. An authentication indicium

$$I=(1, I_1; 2, I_2; \ldots; G, I_G) \quad (31)$$

is associated with the array of rectangles rec_g for the pixel array PA, characterizing the chosen subset CS.

Proceeding by analogy, a parallelogram par_g with fixed interior angles $\phi 1(<90°)$ and $\phi 2=180°-\phi 1$, with base b, overall length λ_x, slant height s and width λ_y is illustrated in FIG. 14, where the ratio r=s/b is fixed. The maximum distance from the parallelogram center C to any pixel location within the parallelogram par_g is given by

$$d_{par,g}=0.5\,[(1+r\cos\phi 1)^2+(r\sin\phi 1)^2]^{1/2}\,b, \quad (32)$$

and the maximum distance $D_{rec,g}$ from any pixel location in the parallelogram par_g, to a pixel location in the chosen subset CS within par_g is then bounded by

$$D_{par,g}\leq 2\,d_{par,g}=[(1+r\cos\phi 1)^2+(r\sin\phi 1)^2]^{1/2}\,b. \quad (33)$$

This upper bound can be raised or lowered by varying the length λ_x. The pixel locations within the parallelogram par_g are consecutively numbered m=1, 2, . . . , $m_{par,g}$, and the sub-indicium I_g is calculated for each parallelogram par_g. An authentication indicium

$$I=(1, I_1; 2, I_2; \ldots; G, I_G) \quad (34)$$

is associated with the array of parallelograms for the pixel array PA, characterizing the chosen subset CS.

The preceding development may be applied to any suitable polygon used as the basis for a set of tesselation polygons TP. The pixel locations may be aligned in a square pattern, as shown in FIGS. 10, 12 and 14, or may be staggered in a diamond pattern, as shown in FIGS. 11 and 13.

The preceding formalism allows the pixel array PA to be covered by an array of polygons of identical shape and size, allows a sub-indicium I_g to be calculated for each of these polygons, and allows an authentication indicium I to be associated with the polygon array for the pixel array PA and the chosen subset CS. This formalism also allows the distance from any pixel location in the pixel array PA to a nearest neighbor pixel location in the chosen subset CS to be bounded above, by a calculable value d_{max} that is proportional to the choice of a single geometric parameter, such as λ_x or λ_y. This upper bound d_{max} can be varied to insure that no pixel in the pixel array PA is more than, say, D=5 pixel-to-pixel units from at least one pixel in the chosen subset CS. With this choice of P, an alteration of the image that is at least P units in width will be detected by the invention. If the nearest neighbor pixel-to-pixel distance is 0.4 mm, for example, this choice of D=5 would detect an image alteration having a width of at least 2 mm. For most purposes, a choice of D in the range 4--100 will provide adequate detection of image alteration. The limit on image alteration width can be raised or lowered by changing the geometric parameter, such as λ_x or λ_y, that determines the size of each of the polygons used for the covering array.

We claim:

1. Apparatus for producing a self-authenticating image, the apparatus comprising:

a digital image camera that forms a digitally expressed image of a selected view as an array of pixel values, with each pixel value corresponding to a pixel in an array of pixels;

position determination means, including a digital computer, for determining position information that includes at least one of the location of the digital camera, the angular orientation of the digital camera and the time at which the digital image camera forms a digitally expressed image; and

digital image storage means for receiving a digital image from the digital image camera, for receiving the position information from the position determination means, for combining the digital image with the position information to form a modified digital image in which each pixel value in a chosen subset CS of the array of pixel values is reformed as a modified array to contain a portion of the position information, for storing this modified array of pixel values, and for providing an authentication key that indicates the chosen subset CS of the array of pixels for which the pixel values have been modified to form the modified digital image.

2. The apparatus of claim 1, further comprising:

authentication means, connected to said digital image storage means, for receiving a putative authentication key and putative position information for a selected digital image, for retrieving from said digital image storage means said position information that was combined with said selected digital image by using said putative authentication key, for comparing the putative position information with said retrieved position information that was combined with said selected digital image, for authenticating said selected digital image if the putative position information substantially agrees with said retrieved position information, and for withholding authentication of said selected digital image if the putative position information does not substantially agree with said retrieved position information.

3. The apparatus of claim 1, further comprising display means, connected to said digital image storage means, for

providing information contained in a modified digital image in at least one of electronically perceptible form, visually perceptible form and audibly perceptible form.

4. The apparatus of claim 1, wherein said position determination means comprises:

a Satellite Positioning System ("SATPS") signal antenna that receives SATPS signals transmitted from at least three SATPS signal sources; and

an SATPS signal receiver/processor to receive and process SATPS signals from the SATPS antenna and to determine the location of the SATPS antenna.

5. The apparatus of claim 1, wherein said position determination means comprises:

at least three SATPS signal antennas, arranged non-collinearly to each receive SATPS signals transmitted from at least three SATPS signal sources; and

an SATPS signal receiver/processor to receive and process SATPS signals from the SATPS antennas and to determine the location of each of the SATPS antennas and the angular orientation of a plane containing at least three of the SATPS antennas and of a selected line lying in this plane, where this selected line has a known angular orientation relative to said digital camera.

6. The apparatus of claim 1, wherein said position determination means comprises:

an SATPS signal antenna that receives SATPS signals transmitted from at least three SATPS signal sources;

an SATPS signal receiver/processor to receive and process SATPS signals from the SATPS antenna and to determine the location of the SATPS antenna; and

angular orientation determination means, attached to said digital camera, for determining the angular orientation of said digital camera at least partly independently of the SATPS signals received from the SATPS signal sources.

7. The apparatus of claim 1, wherein said position determination means comprises:

an SATPS signal antenna that receives SATPS signals transmitted from at least three SATPS signal sources; and

an SATPS signal receiver/processor to receive and process SATPS signals from the SATPS antennas and to determine the times of receipt of the SATPS signals at the SATPS antenna.

8. The apparatus of claim 1, wherein:

(1) said pixel values in said array of pixel values are numbered m=1, 2, . . . , N;

(2) said pixel value number m is assigned a unique prime number p(m) in a sequence of distinct prime numbers;

(3) said pixel value number m is assigned a number q(m)=p(m) if said pixel value numbered m belongs to said chosen subset CS of pixel values and is assigned a number q(m)=1 if said pixel value numbered m does not belong to said chosen subset CS of pixel values; and

(4) said key I is defined by

$$I=\prod_{m=1}^{N} q(m).$$

9. The apparatus of claim 1, wherein:

(1) said pixel bit values in said array of pixel values are numbered m=1, 2, . . . , K·N, where K is the number of bits used to express a pixel value;

(2) said pixel bit value number m is assigned a unique prime number p(m) in a sequence of distinct prime numbers;

(3) said pixel bit value number n is assigned a number q'(m)=p(m) if said pixel bit value numbered m belongs to said chosen subset CS of pixel bit values and is assigned a number q(m)=1 if said pixel bit value numbered m does not belong to said chosen subset CS of pixel bit values; and

(4) said key I is defined by

$$I=\prod_{m=1}^{K\cdot N} q'(m).$$

10. The apparatus of claim 1, wherein:

(1) said pixel values in said array of pixel values are numbered m=1, 2, . . . , N;

(2) said pixel value number m is assigned a number r(m)=1 if said pixel value numbered m belongs to said chosen subset CS of pixel values and is assigned a number r(m)=0 if said pixel value numbered m does not belong to said chosen subset CS of pixel values; and

(3) said key I is defined by

$$I=\sum_{m=1}^{N} r(m)Z^{-m},$$

where Z is a selected real number greater than 1.

11. The apparatus of claim 10, wherein said real number Z is selected to be equal to 2.

12. The apparatus of claim 1, wherein:

(1) said pixel bit values in said array of pixel values are numbered m=1, 2, . . . , K·N, where K is the number of bits used to express a pixel value;

(2) said pixel bit value number n is assigned a number r'(m)=1 if said pixel bit value numbered m belongs to said chosen subset CS of pixel bit values and is assigned a number r'(m)=0 if said pixel bit value numbered m does not belong to said chosen subset CS of pixel bit values; and

(3) said key I is defined by

$$I=\sum_{m=1}^{K\cdot N} r'(m)Z^{-m},$$

where Z is a selected real number greater than 1.

13. The apparatus of claim 12, wherein said real number Z is selected to be equal to 2.

14. The apparatus of claim 1, wherein said authentication means provides an overlay of polygons p_g, numbered g=1, 2, . . . , G (G≧2), of substantially identical shape and size that overlays said array of pixel locations, assigns each pixel location in said array of pixel locations to one polygon in the overlay, assigns at least one pixel location in said chosen subset CS to each polygon in the overlay, computes a sub-key (g,I_g) for each polygon p_g that indicates the members of said chosen subset CS that are assigned to the polygon p_g, and determines said authentication key I from the collection of sub-key $\{(g, I_g)\}_g$ determined for the polygons p_g in the overlay.

15. The apparatus of claim 14, wherein said polygons p_g in said overlay are drawn from a class of polygons consisting of isosceles triangles, equilateral triangles, squares, rectangles, parallelograms, equilateral regular hexagons and non-equilateral regular hexagons.

16. The apparatus of claim 1, wherein said chosen subset CS of said array PA of pixel values is chosen so that, for any pixel in said pixel array PA a circle, centered at this pixel and

having a diameter at least equal to a selected threshold number D, contains at least one pixel belonging to said chosen subset CS, where D is at least four times the pixel-to-pixel nearest neighbor distance.

17. The apparatus of claim 1, wherein said chosen subset CS of said array PA of pixel values includes at least one of the following patterns of pixels: a substantially straight line containing contiguous pixels, a substantially straight line containing non-contiguous pixels, a curved line containing contiguous pixels, and a curved line containing non-contiguous pixels.

18. A method for producing a self-authenticating digital image, the method comprising the steps of:

forming a digitally expressed image of a selected view as an array of pixel values, using a digital camera, with each pixel value corresponding to a pixel in an array of pixels;

determining position information including at least one of the location of the digital camera, the angular orientation of the digital camera and the time at which a digital image was formed;

receiving a digital image from the digital camera;

receiving the position information for the digital image;

combining the digital image with the position information to form a modified digital image in which each pixel value in a chosen subset CS of the array of pixels is reformed as a modified array to contain a portion of the position information, and storing the modified array of pixel values in a digital image storage module; and

providing an authentication key that indicates the chosen subset CS of the modified array of pixels.

19. The method of claim 18, further comprising the steps of:

providing authentication means, connected to said digital image storage module, for receiving a putative authentication key and putative position information for a selected digital image, for retrieving from said digital image storage means said position information that was combined with said selected digital image by using the putative authentication key, for comparing the putative position information with said retrieved position information that was combined with the selected digital image;

authenticating the selected digital image if the putative position information substantially agrees with said retrieved position information; and

withholding authentication of the selected digital image if the putative position information does not substantially agree with said retrieved position information.

20. The apparatus of claim 18, further comprising the step of providing display means, connected to said digital image storage module, for presenting information contained in a modified digital image in at least one of electronically perceptible form, visually perceptible form and audibly perceptible form.

21. The apparatus of claim 18, wherein said step of determining said position information comprises:

providing a Satellite Positioning System ("SATPS") signal antenna that receives SATPS signals transmitted from at least three SATPS signal sources; and

providing an SATPS signal receiver/processor to receive and process SATPS signals from the SATPS antenna and to determine the location of the SATPS antenna.

22. The apparatus of claim 18, wherein said step of determining said position information comprises:

providing at least three SATPS signal antennas, arranged non-collinearly to each receive SATPS signals transmitted from at least three SATPS signal sources; and

providing an SATPS signal receiver/processor to receive and process SATPS signals from the SATPS antennas and to determine the location of each of the SATPS antennas and the angular orientation of a plane containing at least three of the SATPS antennas and of a selected line lying in this plane, where this selected line has a known angular orientation relative to said digital camera.

23. The apparatus of claim 18, wherein said step of determining said position information comprises:

providing an SATPS signal antenna that receives SATPS signals transmitted from at least three SATPS signal sources;

providing an SATPS signal receiver/processor to receive and process SATPS signals from the SATPS antenna and to determine the location of the SATPS antenna; and

providing angular orientation determination means, attached to said digital camera, for determining the angular orientation of said digital camera independently of the SATPS signals received from the SATPS signal sources.

24. The apparatus of claim 18, wherein said step of determining said position information comprises:

providing an SATPS signal antenna that receives SATPS signals transmitted from at least three SATPS signal sources; and

providing an SATPS signal receiver/processor to receive and process SATPS signals from the SATPS antennas and to determine the time of receipt of the SATPS signals at the SATPS antenna.

25. The apparatus of claim 18, wherein said step of providing an authentication key I comprises the steps of:

(1) numbering said pixel values in said array of pixel values m=1, 2, . . . , N;

(2) assigning to said pixel value number m a unique prime number p(m) in a sequence of distinct prime numbers;

(3) assigning to said pixel value number n a number q(m)=p(m) if said pixel value numbered m belongs to said chosen subset CS of pixel values and

(4) defining said key I by

$$I = \prod_{m=1}^{N} q(m).$$

26. The apparatus of claim 18, wherein said step of providing said authentication key I comprises the steps of:

(1) numbering said pixel bit values in said array of pixel values m=1, 2, . . . , N;

(2) assigning to said pixel bit value number a unique prime number p(m) in a sequence of distinct prime numbers;

(3) assigning to said pixel bit value number m a number q'(m)=p(m) if said pixel bit value numbered m belongs to said chosen subset CS of pixel bit values and assigning a number q(m)=1 if said pixel bit value numbered m does not belong to said chosen subset CS of pixel bit values; and

(4) defining said key I by

$$I=\prod_{m=1}^{N} q(m).$$

27. The apparatus of claim 18, wherein said step of providing said authentication key I comprises the steps of:

(1) numbering said pixel values in said array of pixel values m=1, 2, . . . , N;

(2) assigning to said pixel value number m a number r(m)=1 if said pixel value numbered m belongs to said chosen subset CS of pixel values and r(m)=0 if said pixel value numbered m does not belong to said chosen subset CS of pixel values; and

(3) defining said key I by

$$I=\sum_{m=1}^{N} r(m)Z^{-m},$$

where Z is a selected real number greater than 1.

28. The apparatus of claim 27, further comprising the step of selecting said real number Z to be equal to 2.

29. The apparatus of claim 18, wherein said step of providing said authentication key I comprises the steps of:

(1) numbering said pixel bit values in said array of pixel values m=1, 2, . . . , K·N, where K is the number of bits used to express a pixel value;

(2) assigning said pixel bit value number m a number r'(m)=1 if said pixel bit value numbered m belongs to said chosen subset CS of pixel bit values and r'(m)=0 if said pixel bit value numbered m does not belong to said chosen subset CS of pixel bit values; and

(3) defining said key I by

$$I=\sum_{m=1}^{K\cdot N} r'(m)Z^{-m},$$

where Z is a selected real number greater than 1.

30. The apparatus of claim 29, further comprising the step of selecting said real number Z to be equal to 2.

31. The apparatus of claim 18, wherein said step of providing said authentication key I comprises the steps of:

providing an overlay of polygons p_g, numbered g=1, 2, . . . , G (G≧2), of substantially identical shape and size that overlays said array of pixel locations;

assigning each pixel location in said array of pixel locations to one polygon in the overlay;

assigning at least one pixel location in said chosen subset CS to each polygon in the overlay;

computing a sub-key (g,I_g) for each polygon p_g that indicates the members of said chosen subset CS that are assigned to the polygon p_g; and

determining said authentication key I from the collection of sub-keys $\{(g,I_g)\}_g$ determined for the polygons p_g in the overlay.

32. The method of claim 31, further comprising the step of choosing said polygons p_g in said overlay from a class of polygons consisting of isoceles triangles, equilateral triangles, squares, rectangles, parallelograms, equilateral regular hexagons and non-equilateral regular hexagons.

33. The apparatus of claim 18, further comprising the step of choosing said chosen subset CS of said array PA of pixels so that, for any pixel in said pixel array PA a circle, centered at this pixel and having a diameter at least equal to a selected threshold number D, contains at least one pixel belonging to said chosen subset CS, where D is at least four times the pixel-to-pixel nearest neighbor distance.

34. The apparatus of claim 18, further comprising the step of choosing said chosen subset CS of said array PA of pixels to include at least one of the following patterns of pixels: a substantially straight line containing contiguous pixels, a substantially straight line containing non-contiguous pixels, a curved line containing contiguous pixels, and a curved line containing non-contiguous pixels.

* * * * *

US005499294A

United States Patent [19]

Friedman

[11] Patent Number: 5,499,294

[45] Date of Patent: Mar. 12, 1996

[54] **DIGITAL CAMERA WITH APPARATUS FOR AUTHENTICATION OF IMAGES PRODUCED FROM AN IMAGE FILE**

[75] Inventor: **Gary L. Friedman**, Encino, Calif.

[73] Assignee: **The United States of America as represented by the Administrator of the National Aeronautics and Space Administration**, Washington, D.C.

[21] Appl. No.: **449,472**

[22] Filed: **May 24, 1995**

Related U.S. Application Data

[63] Continuation-in-part of Ser. No. 159,980, Nov. 24, 1993, abandoned.

[51] **Int. Cl.**[6] **H04N 7/167**; H04K 1/00; H04L 9/00

[52] **U.S. Cl.** **380/10**; 380/30; 380/18; 348/207; 348/441; 348/460; 348/469; 348/552

[58] **Field of Search** 380/10, 30; 348/207, 348/441, 460, 469, 552

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,453,074	6/1984	Weinstein	235/380
4,670,857	6/1987	Rackman	380/4
4,879,747	11/1989	Leighton et al.	380/23
5,005,200	4/1991	Fischer	380/30
5,027,401	6/1991	Soltesz	380/54
5,185,794	2/1993	Thompson et al.	380/17
5,321,749	6/1994	Virga	380/18

OTHER PUBLICATIONS

Whitfield Diffie, et al., "New Directions in Cryptography," IEEE Trans. on Information Theory., vol. IT-22, No. 6, pp. 644–654, Nov. 1976.

Taher Elgamal, "A Subexponential-Time Algorithm for Computing Discrete Logarithms over GF(p^2)," IEEE Trans. on Information Theory, vol. IT-31, No. 4, pp. 473–481, Jul. 1985.

R. L. Rivest, et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, No. 2, pp. 120–126, Feb., 1978.

Dennis K. Branstad, "The Proposal for a U.S. Standard for Digital Signature Encoding," IEEE Spectrum, pp. 30, Aug. 1992.

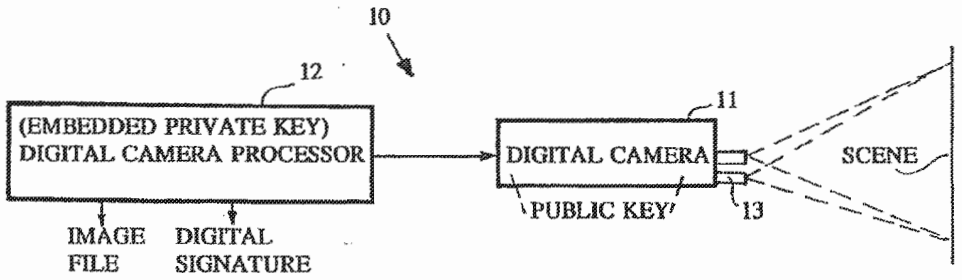
Primary Examiner—Stephen C. Buczinski

Attorney, Agent, or Firm—John H. Kusmiss

[57] **ABSTRACT**

A digital camera equipped with a processor for authentication of images produced from an image file taken by the digital camera is provided. The digital camera processor has embedded therein a private key unique to it, and the camera housing has a public key that is so uniquely related to the private key that digital data encrypted with the private key may be decrypted using the public key. The digital camera processor comprises means for calculating a hash of the image file using a predetermined algorithm, and second means for encrypting the image hash with the private key, thereby producing a digital signature. The image file and the digital signature are stored in suitable recording means so they will be available together. Apparatus for authenticating the image file as being free of any alteration uses the public key for decrypting the digital signature, thereby deriving a secure image hash identical to the image hash produced by the digital camera and used to produce the digital signature. The authenticating apparatus calculates from the image file an image hash using the same algorithm as before. By comparing this last image hash with the secure image hash, authenticity of the image file is determined if they match. Other techniques to address time-honored methods of deception, such as attaching false captions or inducing forced perspectives, are included.

9 Claims, 3 Drawing Sheets



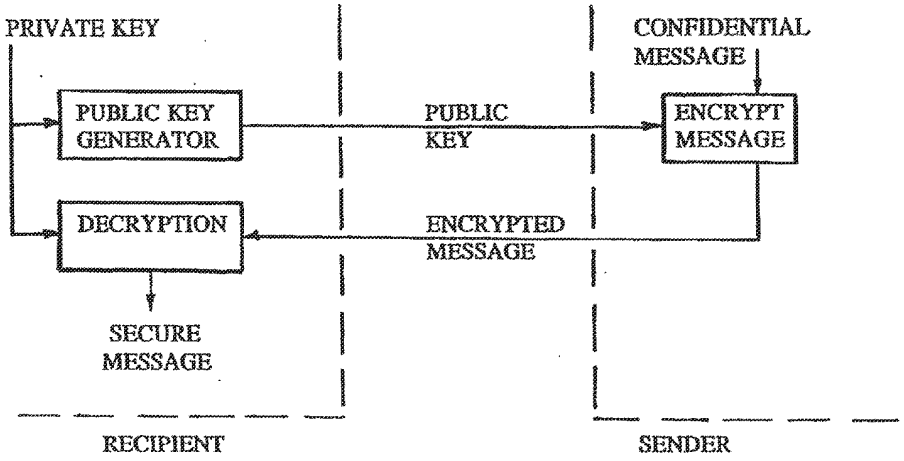


FIG. 1
PRIOR ART

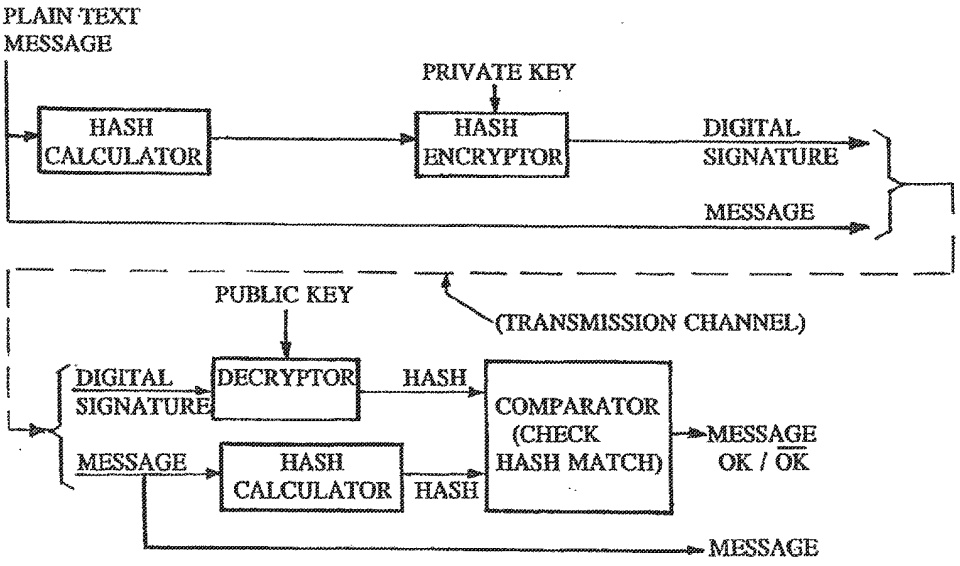


FIG. 2
PRIOR ART

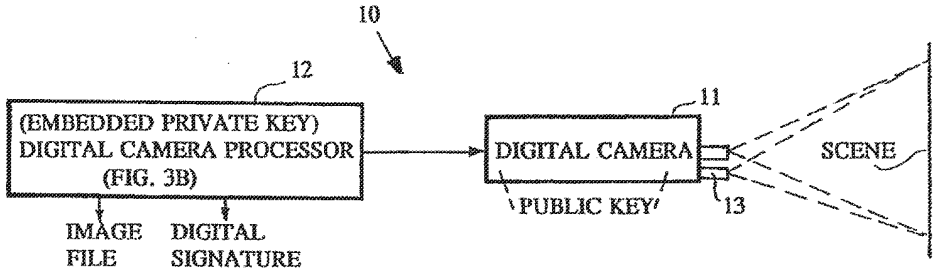


FIG. 3A

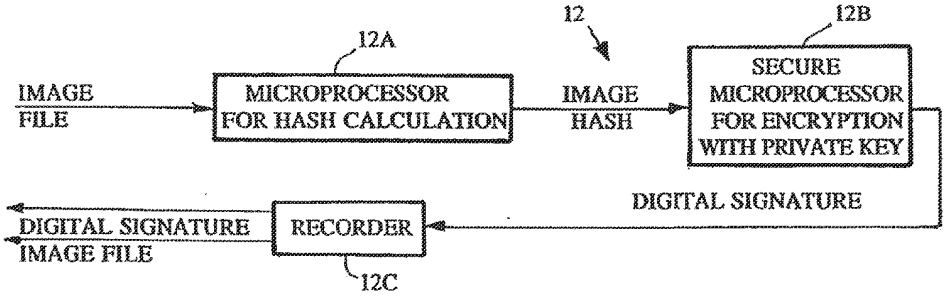


FIG. 3B

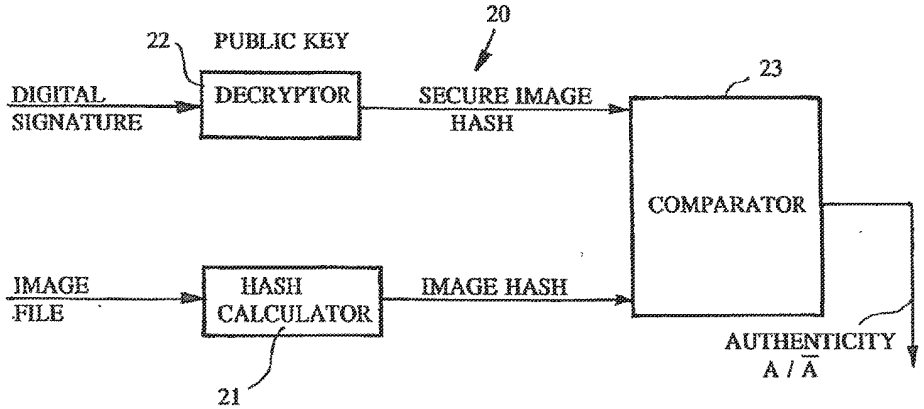
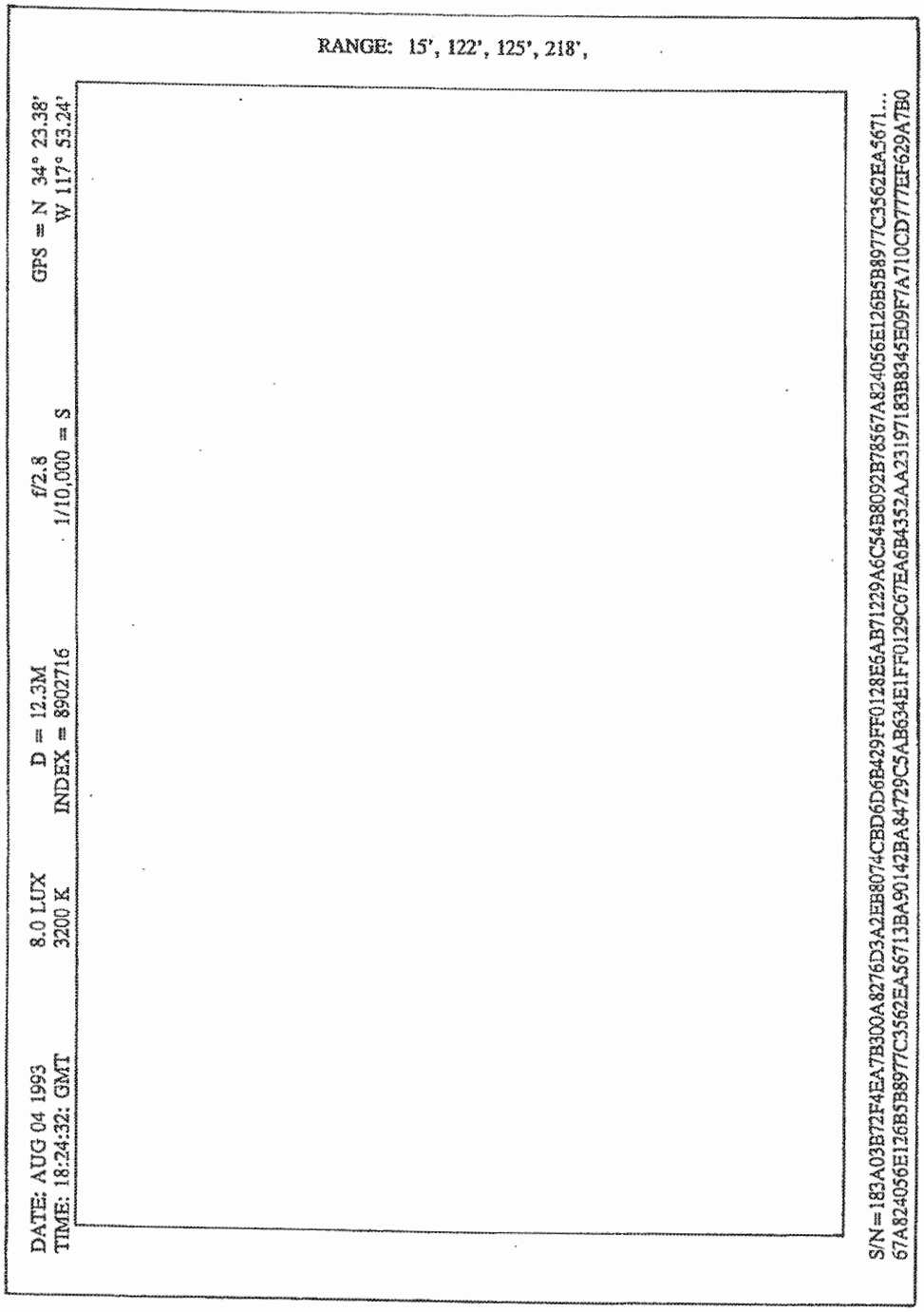


FIG. 3C

FIG. 4



ADOBE – Exhibit 1002, page 249

DIGITAL CAMERA WITH APPARATUS FOR AUTHENTICATION OF IMAGES PRODUCED FROM AN IMAGE FILE

ORIGIN OF INVENTION

The invention described herein was made in the performance of work under a NASA contract, and is subject to the provisions of Public Law 96-517 (35 USC 202) in which the contractor has elected not to retain title.

This application is a continuation-in-part of application Ser. No. 08/159,980, filed Nov. 24, 1993, now abandoned.

TECHNICAL FIELD

The invention relates to the field of photography, and more particularly to a digital camera equipped with apparatus for enabling an image file produced by the camera to be authenticated.

BACKGROUND ART

Photographs have in general been regarded as mediums that "do not lie." However, the inherent trustworthiness of photographs have been compromised by the increasing sophistication and ease with which photographic images can be manipulated. This problem is particularly severe in the case of digital cameras which store a recorded image in digital memory, such as on magnetic tape or laser disc instead of photographic film. There the concept of an "original" image is no longer meaningful.

While a need for authenticating photographs exists today, the seriousness of the problem is not yet widely acknowledged. Consider, for example, that while a photograph can be readily altered to a limited extent, it can be authenticated only to some degree by comparing a positive print with its negative film recorded by a camera while inspecting the negative film for evidence of physical alteration. Authentication of an image recorded by a digital camera is more difficult because there is no physical "original" to compare or negative to examine; furthermore, the digital image file produced by these cameras (as well as other digitally recorded information such as audio and video files) can be easily manipulated using sophisticated computers which make such manipulation easy and, as techniques improve, more difficult to detect.

Today, most pictures that appear in newspapers and magazines have been altered to some degree, with the severity varying from the trivial (such as deliberately removing distracting background while cleaning up "noise") to the point of deliberate deception, such as substituting heads on people's bodies. As the power, flexibility and ubiquity of image-altering computers continues to increase, the notion that photographs "do not lie" will become less widely held.

BACKGROUND ON DIGITAL SIGNATURES

The concept of a digital "signature" is based upon recent encryption techniques called "public key encryption." [Whitfield Diffie and Martin E. Hellman, *"New Directions in Cryptography,"* IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp. 644–654, November, 1976; Taher Elgamal, *"A Subexponential-Time Algorithm for Computing Discrete Logarithms over GF(p^2),"* IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp. 473–481, July 1985; and R. L. Rivest, A. Shamir and L. Adleman, *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,"* Communications of the ACM, Vol. 21, No. 2, pp. 120–126, February, 1978]

Older encryption/decryption schemes require that both the Sender and receiver possess the same secret "key": the sender uses the key to transform the text message into ciphertext, and the receiver uses the same key to perform an inverse transformation on the ciphertext, revealing the original text message. If the correct key transforms the ciphertext into unreadable garbage, it is reasonable to conclude that either the wrong key is being used, the message has been altered, or the sender has been impersonated by someone ignorant of the fact that a key is required to encrypt so the receiver can decipher. The historic drawback to this secret key encryption scheme has been in the secure distribution of keys; disclosure of the key by the sender to the receiver must occur out-of-band, either transmitted via an expensive alternate path or at some prior time, such as when the sender and the receiver were in the same space at the same time.

Public-key encryption techniques differ in that they enable the recipient of a message to decrypt it using a public key that is different from the one used by the sender to encrypt it, but mathematically related to it. Public key encryption employs two different keys: a private key, which is held by the security conscious party sending the message, and a corresponding public key, which need not be kept secret. The public key is generated based upon the private key, making the pair unique to each other.

All public-key cryptography is based on the principle that it is easy to multiply two large prime numbers together, but extremely difficult (taking perhaps centuries using today's supercomputers) to work backwards and uncover the factors (public and private keys) that could have been used to generate the resulting product of the multiplication process.

The public-key scheme is illustrated in FIG. 1 and works as follows: to send a secret message that only the recipient can read, the recipient's public key would first be made known to the sender via any nonsecure medium, such as a letter, a telephone conversation, or a newspaper notice. Anyone wishing to send a secure message would encrypt the message using this public key and transmit it to the recipient. The recipient, having sole possession of the corresponding private key, is the only one able to decrypt the message. The need to transmit a secret key that both parties must possess beforehand is thus obviated. The tradeoff is that, although only the recipient can decrypt the message, anyone who intercepts the public key can send a message with anonymity.

The process described above can also be implemented "backwards" to great advantage. In a second scenario, it is the sender who maintains possession of the private key, and anyone who has the widely disseminated corresponding public key is able to decrypt the message encrypted using the private key. Although this procedure no longer performs the traditional function of encryption (which is to provide confidential communication between two parties), it does provide a way to insure that messages are not forged: only the private key could have produced a message that is decipherable by anyone having the corresponding public key.

The foregoing provides the foundation for the concept of digital signatures; encoding a smaller representation of the message to verify the integrity and source of the message, as will now be described with reference to FIG. 2. The sender of a message generates a unique digital signature by hashing the message using a regular algorithm and encrypting the message using a private key. There is a public key corresponding to the private key to enable decryption of the

hashed message. The digital signature is transmitted along with the plain (unhashed and unencrypted) text message so that a recipient may decrypt the digital signature and thus authenticate the message by comparison of the decrypted hash and a hash of the plain text message transmitted with the signature. Any difference will readily show that the message has been altered or has been transmitted by a person other than the one possessing the private key, which is itself a digital code. Thus, as long as the private key remains private, only the private key holder can produce messages decipherable by anyone holding the public key. Furthermore, it is extremely difficult to "reverse-engineer" the encrypted message using the public key to ascertain the private key. Without knowledge of the private key, a digital "signature" cannot be forged.

Digital signatures thus build upon the public-key cryptographic technique and allow a recipient to not only authenticate the contents of a plain text message but also the identity of the sender without obscuring the original message. Digital signatures are produced by creating a hash of the original plain text message, and then encrypting the hash using the sender's private key, as shown in the top half of FIG. 2. The result is a second, smaller digital file referred to as a signature which accompanies the original plain text message as a separate block of data.

A "hash" is created by a mathematical function which maps values from a large domain into a smaller range. For example, a checksum is a simple kind of hash. A more complex example of a hash algorithm would involve dividing a binary file into a collection of, say, 16 kilobit pieces and performing a cumulative exclusive-OR function between successive pieces. That produces a simple 16 kilobit hash which is smaller than the original file yet is particularly unique to it. Many more complex and secure transformations are also possible. An advantageous characteristic of a hash is that changing a single bit in the original message input would produce a very different hash output if subjected to the same mathematical function. This advantage of a hash will become apparent in the use of a hash in the present invention. Another advantage is that reverse engineering a message so it will yield a given hash and also make sense to the reader is virtually impossible. Thus, a key to the present invention is that a unique encrypted digital signature can be created by encrypting the output of the hashing function using a sender's private key.

In the process of hashing a message to produce a digital signature, the original message is retained unaltered; only the message's hash is altered by encryption with a private key. This way the original file can be read by anyone, yet each recipient may authenticate the message by decrypting the message's unique digital signature using the public key. If the decrypted digital signature and hash of the message in question is created by the same mathematical function that matches, both the integrity of the message and the authenticity of the sender are assured.

DIGITAL CAMERAS

Standard digital cameras are filmless; they sense light and color via an electronic device, such as a charge coupled device commonly known as a CCD, and produce as an output a computer file which describes the image using data bits (1's and 0's) arranged in a meaningful, predefined format. Often this digital image file is first stored on a small mass-storage medium inside the camera itself, such as a magnetic floppy disc, or a magneto-optical disk commonly referred to as a compact disc (CD), for later transference to a digital system for image processing and/or display. Alternatively, the image file can be sent directly to a digital system via a transmission medium. Once inside the digital system, it then can be displayed and easily altered in any number of different ways.

There are several ways of lying with an image, some as old as photography itself. The primary methods are: attaching false captions to the published photograph, using false perspectives and distortions of a scene, and manipulating the appearance of objects or persons in the scene, such as by computer-assisted manipulation of pixels while the image is still stored in digital form. The present invention addresses techniques for thwarting attempts to lie with photographs using one or more of these ways of lying.

STATEMENT OF THE INVENTION

An object of the invention is to provide a solution to the problem of authenticating digital image files, where the image file may be, for example, a single still image from a digital camera, a sequence of images from a digital video camera or even digital holograms. Authentication in this sense means to establish as worthy of belief that the image file has not been altered after its digital signature has been created. The term "image file" is thus used herein to refer to the recorded file of a digital still camera, a digital video camera or a digital holographic camera.

In accordance with one aspect of the invention, a digital camera system is equipped with not only the means for providing an image file (either stored in an internal medium for later transmission or transmitted directly to a digital image processing system) but also means for first providing a hash of the image file or blocks of the file in the case of a very long image file, such as from a video camera and means for then encrypting the hash with a unique private key embedded in the digital camera system. The private key is not known by anyone except perhaps the manufacturer of the digital camera system, or the encrypting means implemented, for example, as a programmed microprocessor embedded in the digital camera system. All that the user need know is a public key unique to the digital camera system. The encrypted hash is stored as a digital signature along with the image file and public key for later authentication.

For authentication of the image file, means for hashing the image file in question produces a checking hash, and means for decrypting the digital signature using the public key reveals the true hash produced by the digital camera system from the true, plain text image file and means for comparing the checking hash with the true hash. If the two hashes match, it is certain that the image file is authentic, i.e., that the image file has not been altered.

To further enhance the authenticatableness of an image from a digital camera system, information is added in a border of the digital camera image frame, such as the public key which is a unique serial number identifying the camera, the date, time, light level, color temperature, f/stop, shutter speed, latitude and longitude of the camera position, the camera pointing direction, focusing distance of the camera lens system and range (distance) from the camera of prominent objects in the image. All of the added information that is recorded in the border of the image frame is hashed and encrypted together with the image to become part of the signature. That information cannot be altered in the original image file containing this information without it being

detected by later comparing the original image file hash with secure image hash of the original image file obtained from the digital signature by decrypting the digital signature with a public key that is mathematically related to the private key. Any alteration of the original image file transmitted with the digital signature, including the information entered on the border of an image file, will result in a mismatch of the two hashes compared. Only if there is not a mismatch will the original image file be declared authentic, and as an additional benefit the source of the image file will be declared as "authentic" since only a source having the private key mathematically related to the public key can produce and send a digital signature that contains a matching hash of the image file hash.

The range information of prominent objects in the digital image scene provides authenticatable data about the scene to an investigator which helps in the identification of inconsistencies in the image as well as in any image caption added to a published photograph or video scene. It also helps prevent use of an altered image that is projected at lifesize proportions and then photographed again with the original camera system at a distance similar to that image's content would suggest for then all objects in the photograph would be recorded as being at virtually the same range since all points in the projected image would be virtually the same as at the center of the projected image

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram illustrating public key encryption.

FIG. **2** is a block diagram illustrating the method of producing and using a digital signature.

FIG. **3***a* illustrates a preferred application of the present invention to digital cameras.

FIG. **3***b* is a block diagram of the present invention as applied to digital cameras for producing a file image with a digital signature to allow authentication of the file image by the recipient.

FIG. **3***c* is a block diagram of a system for authenticating the file image from the digital camera of FIG. **3***a*.

FIG. **4** illustrates a colored border of an image from a digital camera.

DETAILED DESCRIPTION OF THE INVENTION

As applied to digital cameras, the object is to provide a digital signature for an image file as it emerges in digital form from a digital camera system **10** for later authentication as required. To accomplish this, the digital camera **11** produces from a contained processor **12** two output files for each captured image as shown in FIG. **3***a*: the first is an all digital, industry standard format image file representing the captured image. The second would be an encrypted digital signature of the image file produced as shown in FIG. **3***b* by using the camera's unique private key (embedded within the digital camera's secure microprocessor **12***b*) to encrypt a hash of the captured image file (produced by hashing microprocessor **12***a*) for creating an encrypted image hash, thus producing a digital signature which, like the image file, is recorded in a recorder **12***c* of the digital camera system **10**, or transmitted directly to a digital processor's memory for later authenticating and viewing the captured image. It is the responsibility of the user to keep track of the image and digital signature files once they leave the camera **10** since both are required to authenticate the image file.

Once the digital image file and the digital signature are generated and stored on a medium in the camera system and/or transferred into a digital processor memory for processing, the image file's authenticity can be checked at any time thereafter by a decrypting authentication system **20** shown in FIG. **3***c* using a public key taken from the camera name plate or the image's border. The public key can be freely distributed to users for authentication of image files using the authentication system **20**. This authentication system **20** has neither the public nor the private key stored. It requires as inputs the digital image file in question, its accompanying digital signature file, and the public key which is unique to the camera believed to have originated the image and digital signature files. It is perfectly reasonable to use as the public key the camera's serial number appearing on the camera's name plate which is used by the manufacturer to identify the camera for such purposes as warranty repair or replacement. The public key is mathematically related to the private key embedded in the secure microprocessor **12***b* of the digital camera **10** to permit decrypting the digital signature with the public key in the conventional way of encryption and decryption using public and private keys. For image authentication, the image file is hashed for comparison, with the secure image hash obtained by decrypting the digital signature that was encrypted with a private key using the public key. If there are no bit mismatches between the secure image hash and the image hash of the image file, authenticity is confirmed, as will now be described in more detail.

The authentication system **20** calculates its own image file hash using a hash calculator **21** comprising a digital processing system programmed with the same hashing algorithm used in the digital camera (which need not be kept a secret) and a secure image hash using a decryptor **22** comprising a digital processing system with the public key as a second input to decrypt the digital signature. That then reveals the hash originally calculated by the digital camera processor **12** at the time the image was taken. Note that both the hash calculator **21** and the decryptor **22** may be implemented in the same digital processing system **20**. A comparator **23** receives the image hash from the hash calculator **21** and the secure image hash from the decryptor **22**. If these two hashes match, it is certain to any required degree that the digital image in question is indeed identical to what the digital camera system **10** originally produced. If, on the other hand, even one single bit in the image being authenticated has been altered, the two hashes will not even closely match and the image's authenticity will be indicated as not being affirmed by an authenticity output signal $\bar{A}$; otherwise the comparator will indicate authenticity by an output signal A.

If the technique is to be effective (i.e., no false positives or false negatives) and extended to larger data sets such as digital video, or even digital holograms, reliance must be made upon the digital memory file systems of the computer mass storage industry, which has already achieved the ability to store and deliver extremely large binary data sets without errors. On the other hand, analog techniques such as the NTSC encoding on video tape formats are not sufficiently reliable for the present invention. Noncorrected digital formats, such as the popular compact disc (CD), are also not sufficiently reliable. In fact CD recording is so unreliable that CD player manufacturers now utilize special techniques, such as "oversampling" to combat the problem of missed bits. Such techniques introduce a large number of errors upon playback which are normally imperceptible and

therefore unsuitable for the purposes of image authentication in accordance with this invention. Consequently, the present invention is directed to extremely reliable digital recording systems of all kinds.

Measures of Protection

The invention as described above is resistant to forgery attempts since the private key (which is not known to anybody except the manufacturer of the camera) is embedded in a probe-proof microprocessor which itself is deeply integrated into the camera's digital system. Even if some adept person were to disassemble the camera and replace the microprocessor chip with one containing a different key, the digital signature produced thereafter would not be decryptable by any public key published by the manufacturer since the private key must be mathematically related to the public key in the conventional way of public key cryptography, and the only private key that is properly related to the public key could not feasibly be derived from the public key.

The advantages of freely distributing the verification algorithm and valid public keys are great; with the algorithm freely available, verification can become commonplace and routine. No special certification authority need be involved in routine authenticity checks and no angst among the parties involved need be created as a result of image file authenticity being challenged. But the mass distribution of the verification algorithm does carry one danger: it would be possible for someone to create a bogus program which looks, behaves, and has the same file length as the genuine verification algorithm with the only difference being it always proclaims a "hash match" regardless of the authenticity of the image being verified. With the algorithm freely and widely available, this is not a large risk as additional copies of the verification algorithm can be easily obtained from multiple sources and a more reliable authenticity check made using a best two-out-of-three scheme. Alternatively, as a precaution, a digital signature and an image file known to have an altered image may be used to authenticate the algorithm of the authenticator to be used to determine whether or not it has been created to always proclaim a "hash match." When the stakes are high and it is extremely important that the authentication algorithm be known to be genuine, an independent certification authority or the manufacturer of the digital camera could be called upon to provide a copy of their own algorithm and the public key from their list of public keys (camera serial numbers) at the time of authentication.

The algorithm and private key necessary for encrypting the digital signature file from within the digital camera are to be embedded inside a new class of secure microprocessors whose ROM contents cannot be read once the recording system leaves the factory. Because the private key used for encryption is hard-coded into the microprocessor chip by the manufacturer (who must then ensure the private key remains secret), credibility of the recording system's output becomes an extension of that of the manufacturer; the digital signature from the digital camera can be considered to be just as reliable and secure as if the signature had been generated by the manufacturer.

Each digital camera should possess its own unique pair of private and public keys, with the private key etched into the system's secure microprocessor and the public key stored in three places: in a public key list kept by the manufacturer, on the digital camera's name plate itself (which can then also double as the camera's serial number), and in a border as shown in FIG. 4 which contains more data about the captured image as will be discussed in more detail below.

Assigning unique keys to each camera has the benefit of avoiding instant obsolescence which would occur if only one private key were used for all cameras, and that key were to be compromised. An even higher level of security would occur if the manufacturer were to destroy all records of each private key as the cameras are manufactured, since at that point the private key is no longer needed by the manufacturer; only the record of public keys are retained, which could be the same as the assigned serial number as noted above. This would eliminate the possibility of private keys being compromised by industrial espionage or theft.

Finally, regular and free distribution of all valid public keys is desirable to defeat a counterfeiter who has learned of the encryption algorithm employed and has written a program to produce digital signatures based on fictitious private key. Decoding these digital signatures would require the use of a public key not generated by the manufacturer and thus expose them as forgeries at the outset. Freely distributing updated public key lists would make it easy to identify and thwart such attempts. In fact, it is recommended that the public key of the camera be recorded on the border of the image file for use as the public key in the decryptor 22 since alteration of that public key in the image file to be authenticated would result in the declaration by the comparator 23 of a mismatch between the secure image hash from the decryptor 22 and the hash of the image file from the hash calculator 21.

Uses of the Invention

The single most obvious use of the present invention in digital cameras would be in situations where proof of image authenticity is necessary; such as for legal evidence, insurance claims, or intelligence gathering. The inevitable transition to digital cameras and electronically-transmitted images will also make it more difficult for the photographer to protect his image copyright, since electronic images tend to proliferate faster and with less control from the author than the traditional distribution method which places image control in the hands of whoever holds the original negative or transparency. Just as it is common practice today to obtain releases from photographed persons for any published picture containing a recognizable image of the person, it is reasonable that in the future no electronic image will be published without first having authenticated the image using the digital signature of the camera which is registered with the photographer in order to thwart claims that photographs published have been altered and to improve the trustworthiness of all publications and to uphold copyright claims.

This technique need not be limited to still digital images. Because digital signatures can be used to verify any block of digital data in an image file, it can also be implemented in digital video cameras as noted hereinbefore. In all of these devices, a digital signature can be generated and recorded each time the recording process stops or pauses, or after each block of data; each video "take" is hashed, encoded and written at the time it is recorded, or in the case of continuous recording by a digital, video recorder at the time each block is completed by using the technique of multiplexing between a set of three sets of buffers; as one buffer is filled with a block of data, another block of data in a second buffer is hashed and encrypted and a third block of data is recorded in a third buffer at a faster clock rate so that its algorithms are complete in the second buffer in time to transfer the digital signature in a third buffer to a camera bulk storage medium before a multiplexer shifts functions among the set of three buffers for the next block of data. Thus, with a set of three buffers A, B and C, assume A is receiving an image block, B is hashing and encrypting a previous block, and C is transferring an encrypted block into the camera bulk storage medium. During the next block interval, the func-

tions are switched A to B, B to C and C to A, and during the third block interval the functions are again switched B to C, C to A, and A to B. The following block interval commences a new multiplexing cycle. In that manner, real-time recording in the camera bulk storage medium is delayed by only three block intervals.

A Special Border

In the case of the digital camera equipped with the present invention being targeted towards legal authentication, a few additional features can be implemented to better serve this use. A brightly colored border could automatically be generated as part of each captured image file. Within the border would appear (as shown in FIG. 4) textual information about the image: the camera public key, the date and time it was taken, the ambient light level seen by the camera at the time of exposure, the original color temperature of the scene, the software version of the camera's firmware, f/stop and shutter speed (or the CCD equivalent "sample time"), the focusing distance of the lens at the time of exposure, the distance (range) of prominent objects in the scene being imaged using a range finder **13**, such as an acoustic, infrared or laser range finder or other range finders such as multiple-object optical range finding or contrast detection range finding systems, a unique image sequence number and, when the technology allows for a Global Positioning System (GPS) receiver to be built into the camera, the geographical coordinates of the camera indicating where in the world the picture was taken.

The present invention as it applies to authentication of camera photographs as described with reference to FIGS. **3***a*, **3***b*, **3***c* and 4 completely mitigates the new threats of computer-assisted alteration of digital image files and eliminates the threat of deception by attaching or substituting false captions or other information recorded in the border as shown in FIG. 4. Such information helps an investigator identify and interpret information by what is depicted in the photographs.

One piece of information captured in the border of the photographs is a record of the distance at which the lens was focused. A second piece of information captured in the border that may be useful in interpretation of the photograph in a more sophisticated way is range information of prominent objects in the scene at the time the picture was taken using the range finder **13**, such as an acoustic range finder, or an infrared or laser range finder. Optical range finders could also be used. In an acoustic range finder, the acoustic module (sometimes referred to as an "ultrasonic transducer" operates at frequencies selected beyond the range of human hearing, and often pulses of multiple frequencies may be used to guard against the absorption of a single frequency by a particular object. Once the timing of the return echo has been obtained, the distance can be determined by employing the formula d=(1,100 t)2 where the distance of the object d is in feet and the t is the number of seconds. For example, if the echo returns in 9 milliseconds, the distance of an object would be recorded as 5 feet. Listening for multiple echoes could allow for recording the distance of several prominent objects in the field of view (typically at least three). Less prominent objects could return echoes of lesser energy, but prominent objects should be selected by adjustment of a threshold selection amplifier. Range information recorded in the image border not only makes digital manipulation of the photograph in a computer more difficult without the manipulated photograph being declared not authentic by the comparator **23**, but also aids one viewing and analyzing the scene with some perspective of the two-dimensional photograph of a three-dimensional scene, such that the depths of all other objects may be estimated by the relative positions of the prominent objects the range of which are determined and recorded.

The range information also thwarts attempts to make a duplicate "original" image file which has been manipulated by projecting at lifesize proportions the manipulated image file and photographing it with the same camera as was used to record the truly original image file at a distance similar to what the image's content would suggest. Such a manipulated duplicate "original" would be readily declared to be not authentic since all ranges recorded for the objects in the image would be virtually the same as the range recorded for objects at or near the center of the projected image instead of the true original ranges recorded in the truly original image file.

The lens' focused distance and f/stop are there to help detect potential abuse of the camera, such as taking a close-up picture of a modified photograph and trying to pass it off as an unaltered original. The ambient light level and color temperature readings would be useful for getting a feel for exactly what the scene was like at the time of exposure; something a sensitive optical element might inadvertently hide via automatic exposure and color correction.

Since all the textual data in the image file border are part of the authenticated image file, their credibility are also upheld when authenticated by the authentication process. The accuracy of the date and time information would again be the responsibility of the secure microprocessor; in addition to being able to keep its algorithm and private key a secret, it also could have a lithium battery powering a system clock set to Universal (Greenwich Mean) Time at the time of manufacture. If the timer should ever fail or is tampered with, the system would be programmed to fill the time and date fields with XXXX's, eliminating the chance of an erroneous random time being indicated for the actual time.

Higher Level of Security

Although the present invention offers a satisfactory level of security, nevertheless there still exists a small possibility that a determined person may be able to discover the camera's private key given an extended amount of time. (No cryptographic scheme will protect data forever; given sufficient time, advancements in code breaking or improved computer power may some day be enough to render any existing level of cryptographic protection obsolete.) If the discovered private key were to be available to the custodian of the camera image files, it would allow the custodian of the image files from that camera to generate authentic-looking digital signatures on altered image files, essentially undermining the credibility offered by the compromised camera. However, the security level of other cameras in use, and of images taken with those other cameras will remain uncompromised.

It would be wise for a manufacturer of such digital cameras to regularly upgrade and enhance the sophistication of the encryption implementation as newer camera models are introduced, typically those using longer encryption/decryption key lengths and improved encryption/decryption and hash algorithms. It is expected that evolving authentication algorithms (the public domain component of this authentication invention which is to be freely distributed) will be designed to be compatible with earlier versions, i.e., to recognize, identify and authenticate image files made with all previous digital camera models equipped with a microprocessor for hash calculation and a secure microprocessor for encryption with a private key.

Because the encryption details must necessarily be changed often (depending on the technological capabilities

of the day), no single image format, key length encryption, or hashing algorithm is being specified. Instead, reference is made to the National Institute of Standards and Technology's (NIST) proposed Digital Signature Standard (DSS) as an example for implementation of the present invention. [Dennis K. Branstad, *"The Proposal for a U.S. Standard for Digital Signature Encoding,"* IEEE Spectrum, pp. 30, August 1992]

A specific application of the present invention is directed toward the solution of an ever more troubling social problem, namely the eroding credibility of photographic images, but its many other applications where image files are to be stored, transmitted and/or transformed to visual form may also benefit from it.

Although particular embodiments of the invention have been described and illustrated herein, it is recognized that modifications may readily occur to those skilled in the art. Consequently, it is intended that the claims be interpreted to cover such modifications and equivalents thereof.

I claim:

1. A digital camera with apparatus for authentication of images produced from an image file taken by said digital camera of a scene, said digital camera having embedded therein a private key unique to said digital camera and a known public key so uniquely based upon said private key that digital data encrypted with said private key may be decrypted using said public key, said digital camera apparatus comprising

first means for calculating image hash of said image file using a predetermined algorithm,

second means for encrypting said image hash with said embedded private key, thereby producing a digital signature uniquely associated with said image file, and

third means for maintaining association of both said image file and said digital signature derived from said image file by said first and second means.

2. A combination as defined in claim 1 including separate apparatus for authenticating at any time said image file as being free of any alteration using said associated digital signature, said separate apparatus comprising

fourth means for decrypting said digital signature, using said public key, thereby deriving a secure image hash identical to said image hash produced by said first means of said digital camera apparatus by calculating image hash of said image file from said digital camera,

fifth means for calculating image hash of said image file that has been maintained in association with said digital signature, said fifth means using said predetermined algorithm, and

sixth means for comparing said image hash of said image file calculated by said fifth means with said secure image hash from said fourth means to determine authenticity of said image file that has been maintained in association with said digital signature for use of said image file in reproducing an image represented by said image file if both said image file and said secure image file match identically.

3. A combination as defined in claim 1 wherein said private key is embedded in said second means.

4. A combination as defined in claim 3 wherein said public key is published.

5. A combination as defined in claim 4 wherein said public key is published on said digital camera.

6. A combination as defined in claim 4 wherein said public key is digitally recorded in a border of said image file and is processed through hashing and encryption with said image file.

7. A combination as defined in claim 6 wherein further information is digitally recorded in said border regarding parameters of said digital camera extant at the time said image file is taken and is processed through hashing and encryption with said image file to assist in reproduction and interpretation of a reproduced image of said scene.

8. A combination as defined in claim 1 wherein focusing distance is digitally recorded in a border of said image file and is processed through hashing and encryption with said image file.

9. A combination as defined in claim 1 wherein range from said digital camera to one or more prominent objects in said scene are recorded in a border of said image file and is processed through hashing and encryption with said image file.

* * * * *

Notice of References Cited	Application/Control No. 09/626,044	Applicant(s)/Patent Under Reexamination JAFFE ET AL.	
	Examiner Hosuk Song	Art Unit 2136	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,253,337	06-2001	Maloney et al.	714/38
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

ADOBE – Exhibit 1002, page 256
JAFFE-ADOBE000290

US006253337B1

(12) **United States Patent**
Maloney et al.

(10) **Patent No.: US 6,253,337 B1**
(45) **Date of Patent: *Jun. 26, 2001**

(54) **INFORMATION SECURITY ANALYSIS SYSTEM**

(75) Inventors: **Michael P. Maloney**, Severna Park; **John M. Suit**, Pasadena, both of MD (US); **Christopher J. Scott**, Pleasant Gap, PA (US); **Francis M. Woodus**, Owings Mills, MD (US)

(73) Assignee: **Raytheon Company**, Lexington, MA (US)

(*) Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/357,539**

(22) Filed: **Jul. 19, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/093,551, filed on Jul. 21, 1998.

(51) **Int. Cl.**[7] **G06F 11/30**

(52) **U.S. Cl.** **714/38**; 714/57; 714/46; 717/4; 713/188

(58) **Field of Search** 714/38, 57, 46, 714/47, 48, 26; 713/201, 188; 717/4

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,361,359	11/1994	Tajalli et al.	395/700
5,410,648 *	4/1995	Pazel	395/158
5,414,833 *	5/1995	Hershey et al.	395/575
5,440,723	8/1995	Arnold et al.	395/181
5,537,540 *	7/1996	Miller et al.	395/183.14
5,555,419	9/1996	Arsenault	395/700
5,608,854	3/1997	Labedz et al.	395/141
5,684,945	11/1997	Chen et al.	395/182.18
5,794,046	8/1998	Meier et al.	395/704

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

409171460A	6/1997	(JP) .
WO 98/42103	9/1998	(WO) .

OTHER PUBLICATIONS

Author Unknown, "Visualization of Network Attacks", Internet site: http://microelec.eng.morgan.edu/~web/network_viz/netviz.htm.*

PCT International Search Report dated Dec. 2, 1999 for PCT/US99/12394 dated Jul. 20, 1999.

PCT International Search Report dated Dec. 1, 1999 for PCT/US99/16467 dated Jul. 20, 1999.

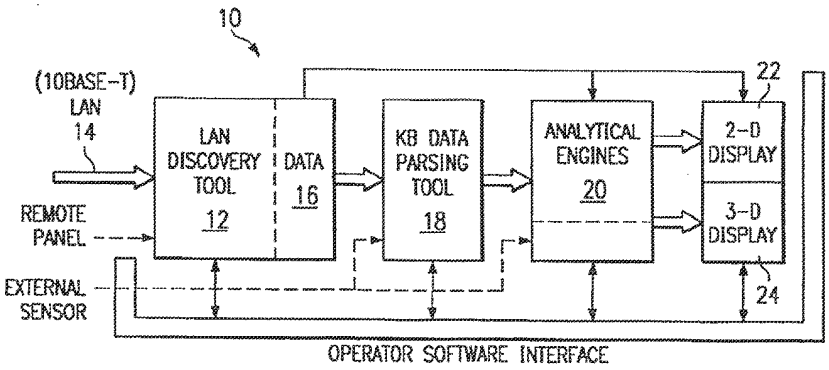
(List continued on next page.)

Primary Examiner—Robert Beausoleil
Assistant Examiner—Scott Baderman
(74) *Attorney, Agent, or Firm*—Baker Botts L.L.P.

(57) **ABSTRACT**

The analysis system is a collection, configuration and integration of software programs that reside on multiple interconnected computer platforms. The software, less computer operating systems, is a combination of sensor, analysis, data conversion, and visualization programs. The hardware platforms consist of several different types of interconnected computers, which share the software programs, data files, and visualization programs via a Local Area Network (LAN). This collection and integration of software and the migration to a single computer platform results in an approach to LAN/WAN monitoring in either a passive and/or active mode. The architecture permits digital data input from external sensors for analysis, display and correlation with data and displays derived from four major software concept groups. These are: Virus Computer Code Detection; Analysis of Computer Source and Executable Code; Dynamic Monitoring of Data Communication Networks; 3-D Visualization and Animation of Data.

20 Claims, 7 Drawing Sheets



U.S. PATENT DOCUMENTS

5,796,951		8/1998	Hamner et al.	395/200
5,819,094	*	10/1998	Sato et al.	395/704
5,822,535		10/1998	Takase et al.	395/200.56
5,832,208	*	11/1998	Chen et al.	713/201
5,845,081		12/1998	Rangarajan et al.	395/200.54
5,923,849		7/1999	Venkatraman	395/200.54
5,958,010		9/1999	Agarwal et al.	709/224
5,960,170	*	9/1999	Chen et al.	395/183.14
5,960,439		9/1999	Hamner et al.	707/103
5,991,881		11/1999	Conklin et al.	713/201
6,026,442		2/2000	Lewis et al.	709/229
6,043,825		3/2000	Glenn et al.	345/440
6,076,106		6/2000	Hamner et al.	709/223
6,088,804	*	7/2000	Hill et al.	713/201

OTHER PUBLICATIONS

Deri L. Mankis D., *"VRML: Adding 3D to Network Management"*, 4th International Conference on Intelligence in Services and Networks, pp. 469–477, May 27–29, 1997.

Law A M et al, *"Simulation Software for Communications Networks: The State of the Art,"* IEEE Communications Magazine, vol. 32, No. 3, pp. 44–50, Mar. 1, 1994.

Chang C K; Al–Saloan Y Y; Defanti T, *Scientific Visualization: A Performance Study of CSMA/CD with Connected Data Links*—(Hybrid–Ethernet), Proceedings of the Third Workshop on Future Trends of Distributed Computing Systems, pp. 389–394, Apr. 14–16, 1992.

PCT International Search Report dated Nov. 17, 1999 for PCT/US99/12393 dated Jul. 20, 1999.

Sczepansky A, *"Auf Herz Und Nieren Pruefen"*, Elektronik, De, Franzis Verlag GMBH, pp. 78–81, Apr. 2, 1997.

Yau S S et al, *"An Interactive Software Maintenance Environment,"* AFIPS Conference Proceedings, pp. 553, 555–561, Jun. 1987.

Lo R et al, *"Towards a Testbed for Malicious Code Detection,"* Computer Society Annual Conference, p. 160–166, 1991.

Saito T et al, *"Protection Against Trojan Horses by Source Code Analysis,"* Electronics & Communications in Japan, Part III—Fundamental Electronic Science, pp. 11–18, Jan. 1994.

* cited by examiner

FIG. 1

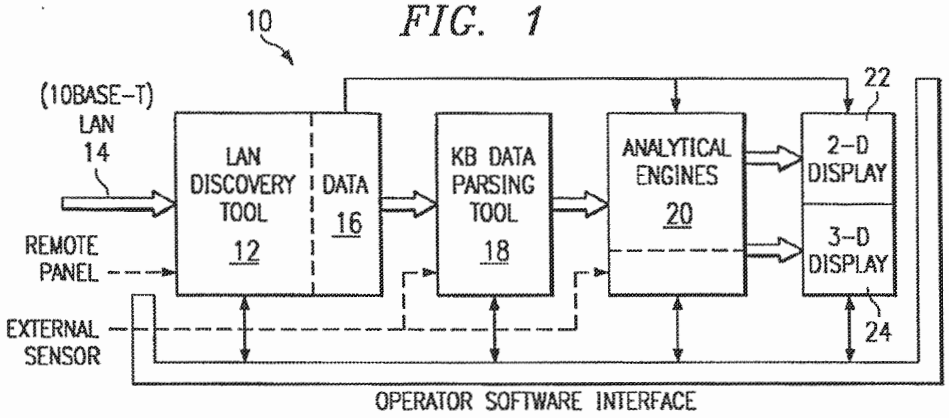

10
(10BASE-T)
LAN
14
REMOTE
PANEL
EXTERNAL
SENSOR
LAN
DISCOVERY
TOOL
12
DATA
16
KB DATA
PARSING
TOOL
18
ANALYTICAL
ENGINES
20
22
2-D
DISPLAY
3-D
DISPLAY
24
OPERATOR SOFTWARE INTERFACE

FIG. 6

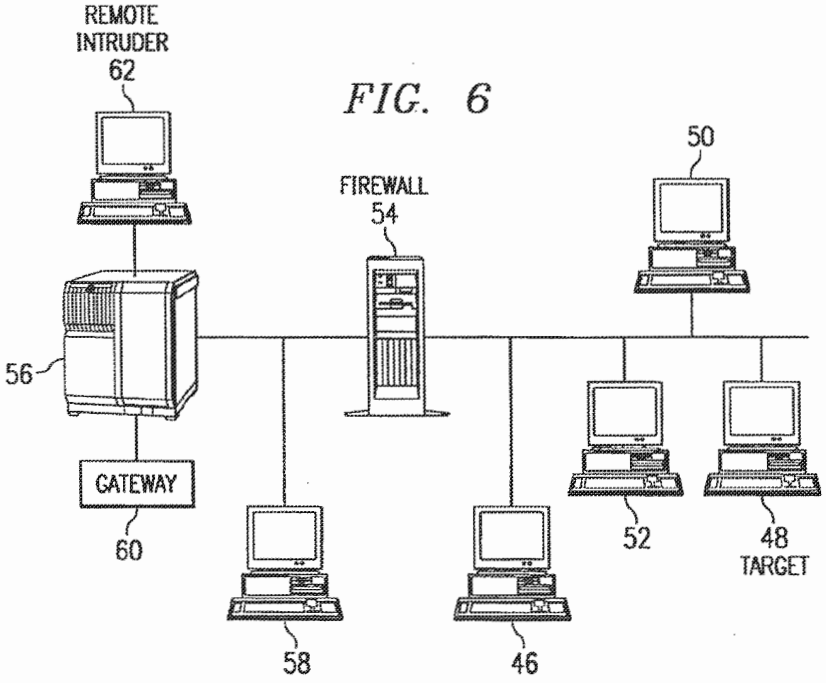
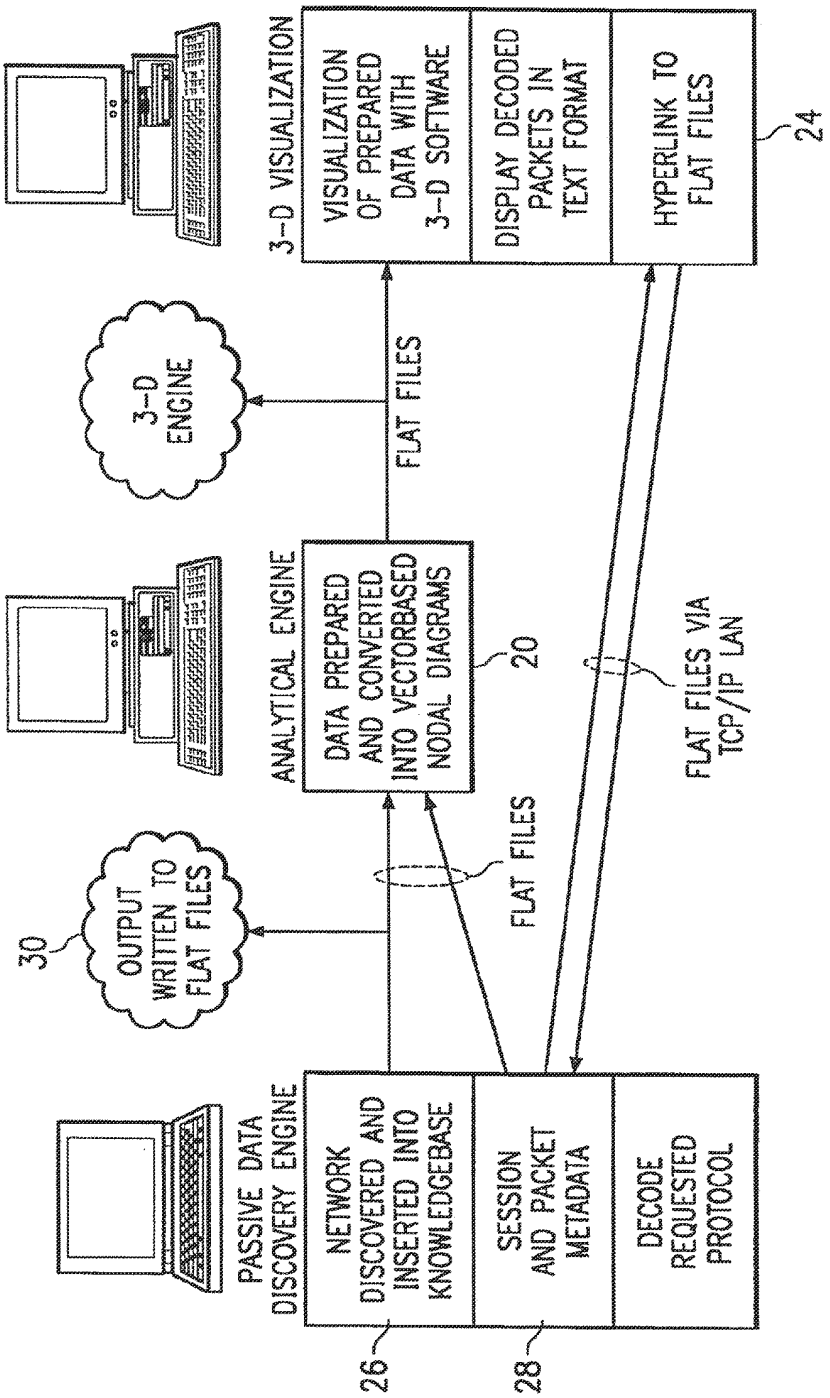
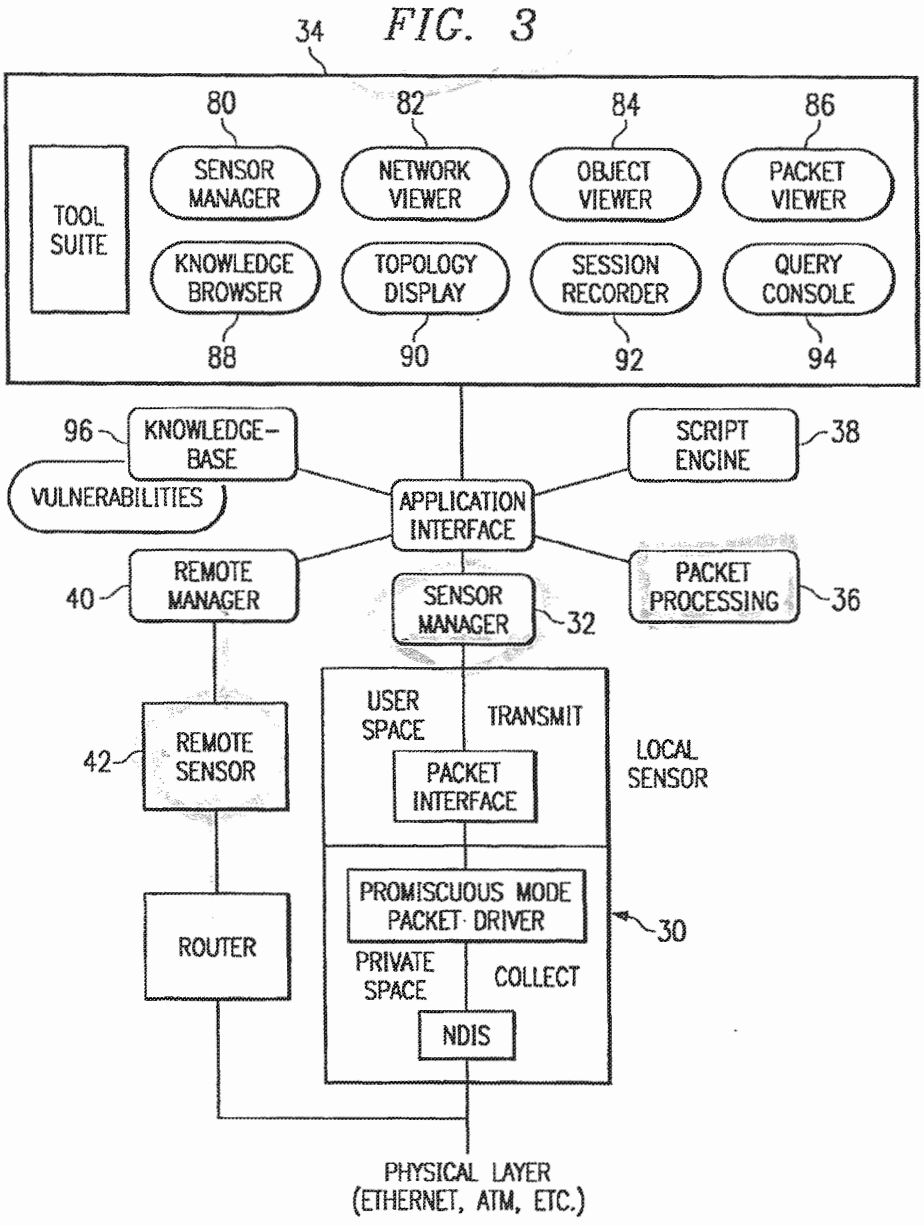

REMOTE
INTRUDER
62
FIREWALL
54
50
56
GATEWAY
60
58
46
52
48
TARGET

FIG. 2



ADOBE – Exhibit 1002, page 260

FIG. 3


34
80
82
84
86
TOOL SUITE
SENSOR MANAGER
NETWORK VIEWER
OBJECT VIEWER
PACKET VIEWER
KNOWLEDGE BROWSER
TOPOLOGY DISPLAY
SESSION RECORDER
QUERY CONSOLE
88
90
92
94
96
KNOWLEDGE-BASE
VULNERABILITIES
SCRIPT ENGINE
38
APPLICATION INTERFACE
REMOTE MANAGER
40
SENSOR MANAGER
32
PACKET PROCESSING
36
USER SPACE
TRANSMIT
LOCAL SENSOR
42
REMOTE SENSOR
PACKET INTERFACE
PROMISCUOUS MODE PACKET DRIVER
30
ROUTER
PRIVATE SPACE
COLLECT
NDIS
PHYSICAL LAYER
(ETHERNET, ATM, ETC.)

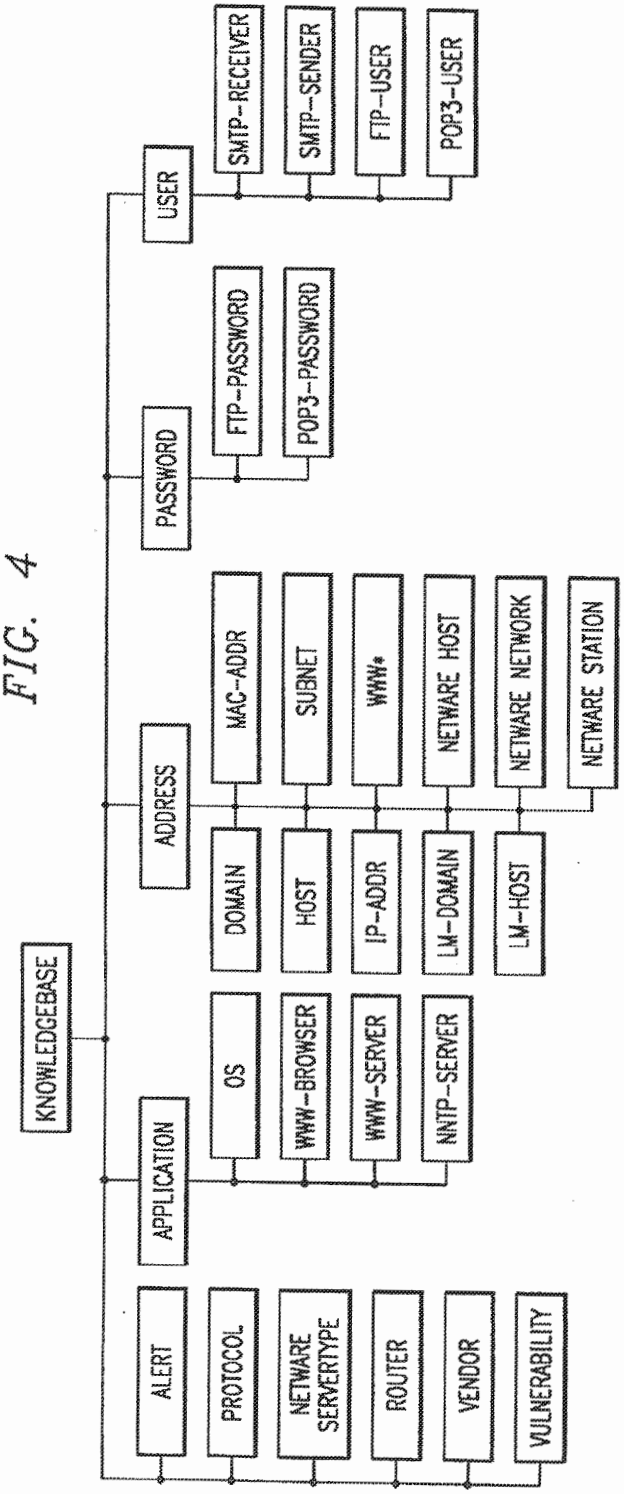


FIG. 4

ADOBE – Exhibit 1002, page 262

JAFFE-ADOBE000296

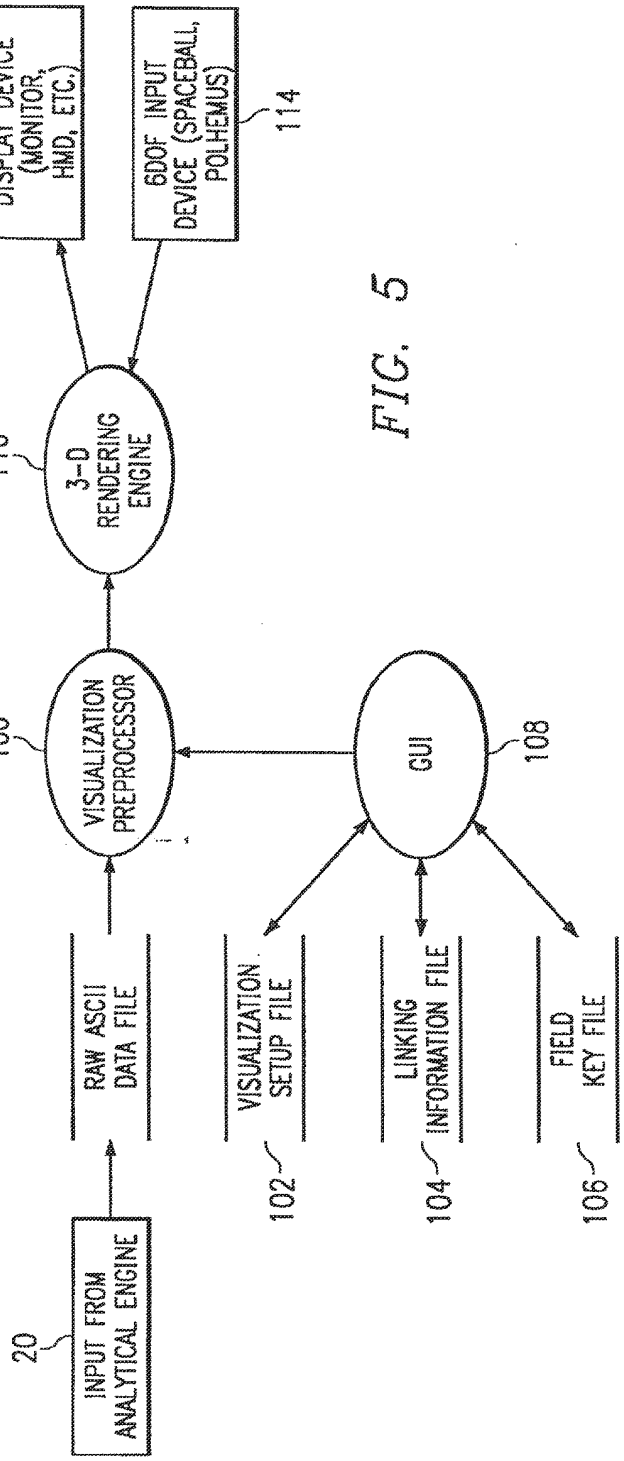
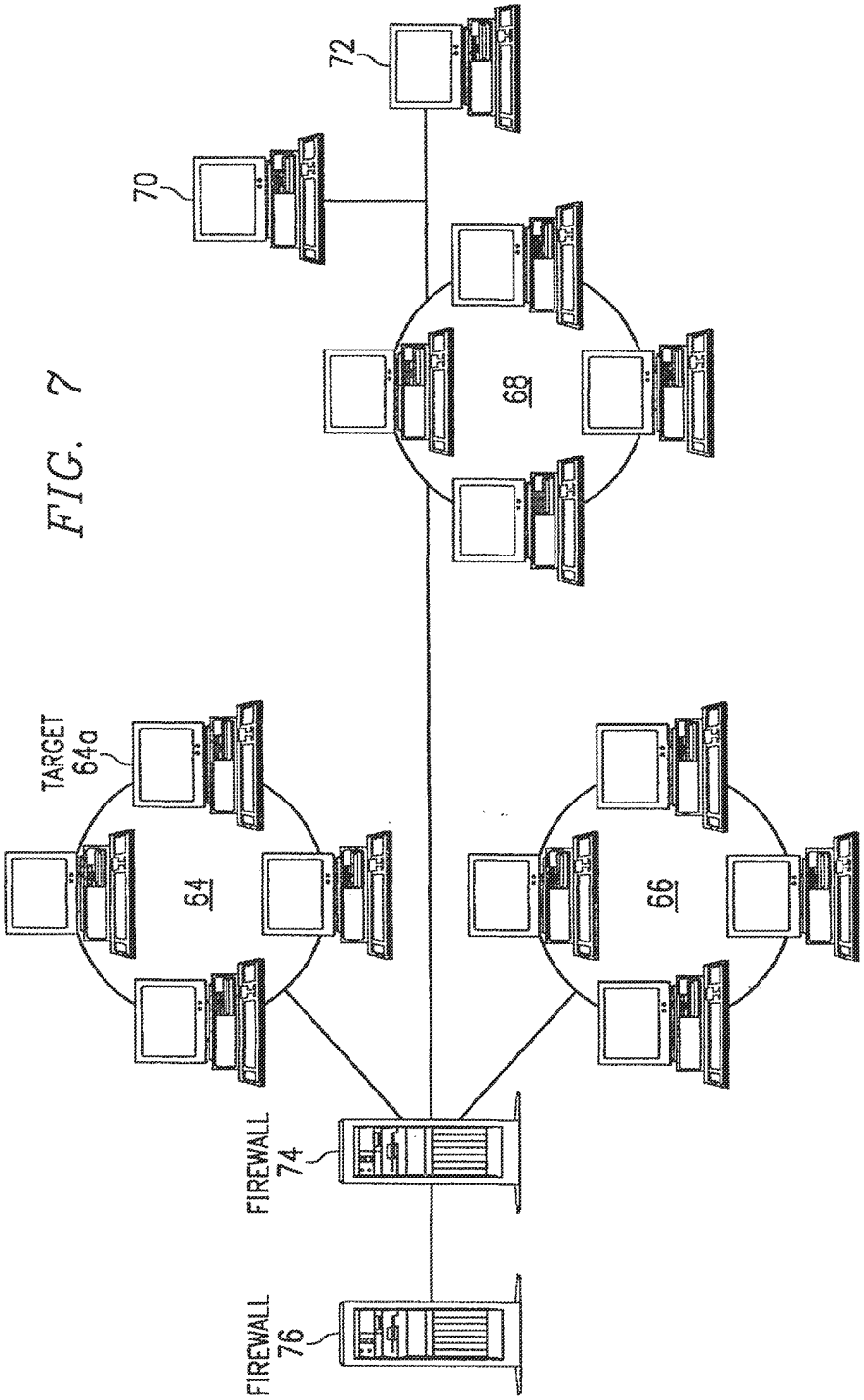


FIG. 5

ADOBE – Exhibit 1002, page 263

FIG. 7



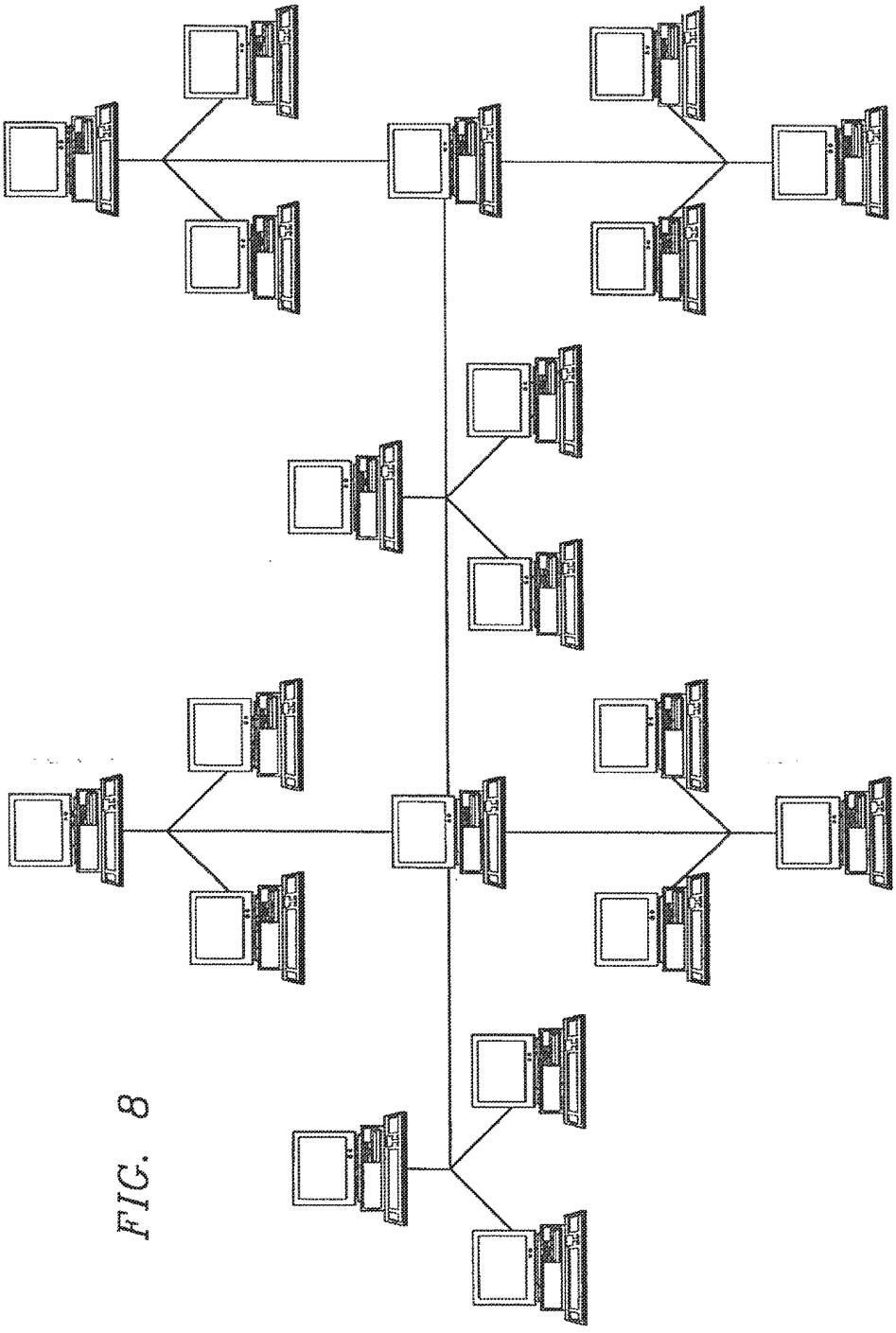


FIG. 8

INFORMATION SECURITY ANALYSIS SYSTEM

RELATED APPLICATION

This application claims the benefit of U.S. provisional application Ser. No. 60/093,551, filed Jul. 21, 1998, entitled Information Security Analysis System.

TECHNICAL FIELD OF THE INVENTION

This invention relates to an information security analysis system for mitigation of Internet security issues and computer source and executable code visualization problems. In particular, the invention relates to an information security analysis system for passive discovery of an intranet equipment configuration vulnerability assessment, and intrusion detection.

BACKGROUND OF THE INVENTION

Worldwide Internet usage continues to grow at a phenomenal rate. Users include governments, institutions, businesses, and individuals, all of which have connected to the Internet for the purpose of conducting daily activities. Unfortunately, the development and implementation of security measures designed to make Internet connection a secure means of communication have not kept pace with the technological advances in the expansion of network development and interconnectivity. As a result Internet users and networks risk having their information compromised by hackers and malicious users who continue to find ways to exploit and subvert networks and data.

Used appropriately, firewall technologies can help to secure the "front door" of corporate intranets, but these technologies have trouble keeping pace with the applications, services and security that users demand. Although many products have been developed that facilitate network topology discovery, few of these are able to act passively.

Intranet security and monitoring needs are continuing to increase in both government and private industry. This is substantiated almost daily in trade publications and Internet news groups. More concrete proof of this resides in the increased requirements for security related skills outlined in government requests for proposals. Both government and private industry are spending significant amounts of time and money to address intranet mapping, monitoring, intrusion detection and computer security. This has lead to a prolific amount of organizations, offering to provide intranet computer security services, analysis tools, and associated products.

SUMMARY OF THE INVENTION

The system of the present invention acts passively and provides a methodology for performing a detailed analysis of data observed during a monitoring session.

Without introducing additional traffic on a network, the system of the present invention produces a virtual picture of network usage and network vulnerabilities. By organizing the inputs of multiple collection tools into visual schematics, Security Administrators become proactive in assessing network weaknesses and in identifying optimum locations for implementing security measures. With the information revealed by the system of the present invention, Security Administrators can identify potential traffic bottlenecks, locate the existence of backdoors, reduce bandwidth usage, develop profiles of users, and pinpoint illicit activity.

The software system of the present invention includes four interconnected modules: passive network discovery, network data recording, network data parsing, and network data analysis tools. Network data visualization capabilities are contained within the passive network discovery and network data analysis modules. The software system enables computer code analysis and the 3-D visualization and animation of network traffic and structure. Optional plug-ins further expand and enhance the software capabilities, thus allowing the software system to remain current regardless of network evolution.

The system of the present invention enables a system administrator to map the network, determine normal and abnormal usage patterns, locate virus attacks, manage network allocation, and display the network.

More technically, the analysis system is a collection, configuration and integration of software programs that reside on multiple interconnected computer platforms. The software, less computer operating systems, are a combination of sensor, analysis, data conversion, and visualization programs. The hardware platforms consist of several different types of interconnected computers, sharing the software programs, data files, and visualization programs via a Local Area Network (LAN). It is this collection and integration of software and the migration to a single computer platform that results in an approach to LAN/WAN monitoring in either a passive and/or active mode. For example, router and firewall software can be monitored in near real time to determine if the code has been functionally changed regardless of security precautions. LAN/WAN data contained in the protocols from the Data Link to Presentation layers in the OSI model are available for analysis with associated displays in two and three-dimensional space.

The architecture also enables digital data input from external sensors for analysis, display and correlation with data and displays derived from four major software groups. These are: Virus Computer Code Detection; Analysis of Computer Source and Executable Code; Dynamic Monitoring of Data Communication Networks; 3-D Visualization and Animation of Data.

The present analysis system templates and displays virus computer code in a graphical functional mode. Current techniques rely on bit stream or real-time monitoring to detect a computer virus in the host computer. The approach of the analysis system of the present invention examines the functionality of suspect code to determine if a computer virus is present prior to its execution in the host computer. The approach can be viewed as deriving a genetic structure and then determining if the genetic structure is resident, for example, in a computer program, file, or e-mail attachments.

Further, the analysis system of the present invention graphically displays and performs comparisons between like types of computer source and executable code in multi-dimensional space to determine if the code has undergone single or multiple functional alterations. The analysis system enables graphical analysis, code sequencing, and comparison of two or more similar source and/or executable computer programs to determine the degree of functional alteration. This can document, graph, animate, dynamically explore and determine functionality in a single computer source or executable program. The system of the present invention is also capable of sorting source and executable code by language and displaying the results in a graphical functional format. For example, a router's filter table file can be monitored periodically to determine if the file has been functionally changed regardless of current standard security precautions.

The analysis system of the present invention passively discovers the physical and virtual characteristics of digital data communication networks and simultaneously displays different digital communication networks in an interactive manner. Virtual discovery is defined as the ability to determine how the digital data network is being used by its participants and who is connecting to whom at any point in time. This process also determines the configuration changes in a digital data communication network over selectable time intervals. The physical presence of the analysis system of the present invention, in the passive mode, on a LAN/WAN system is undetectable when using conventional techniques, requires no user privileges, consumes no network bandwidth, and does not interfere with communications on LAN/WAN systems. The analysis system can quickly map SubNets and build complete networks as terminal activity increases. Each active terminal target in the network is mapped and displayed along with appended information. The displayed information shows both physical and virtual relationships, as well as network representations. The analysis system can also be combined with network probes to form remote monitoring, collaboration and discovery of LAN systems. In this scenario, a terminal acts as a master unit with input from the remote probes. In this mode of operation a passive mode of operation may or may not cease depending on whether collaboration is in-band and/or out-of-band.

The analysis system of the present invention dynamically displays, rotates, and animates any data it receives from the three major software groups in three or more dimensions. Simultaneous viewing of different types of digital data in either a physical and/or virtual realms is available.

In accordance with the present invention, the connectivity and functionality for each type of digital data is displayed. The data from each of the three major software groups can be displayed and rotated on any axis on two or more separate but connected visual plains. The process also displays connectivity between different types of data from the three major software groups to include data input from external sensors. The visualization software can append user definable symbols for easier understanding by an operator or analyst. The software interacts with a node via a "mouse click" and dynamically retrieves, decodes and displays information relating to the node that is represented by the three major software groups. In the event that the 3-D nodal diagrams become cluttered, the analyst contracts several nodes into single interconnecting common nodes. This capability provides an uncluttered representation of the original diagram for the analyst while maintaining functionality of the individual contracted nodes.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the present invention may be had by reference to the following detailed description when taken in conjunction with the accompanying drawings wherein:

FIG. **1** is a block diagram of an information security analysis system for passive network data discovery, visualization and analysis in accordance with the present invention;

FIG. **2** is an application flow diagram of the information security analysis system of FIG. **1**;

FIG. **3** is a block diagram illustrating the architecture for a discovery tool for use with the information security analysis system of FIG. **1**;

FIG. **4** schematically represents a typical information structure for the discovery tool illustrated in FIG. **3**;

FIG. **5** is a block diagram of the 3-D visualization module of the information security analysis system of FIG. **1**;

FIG. **6** is a block diagram of the information security analysis system of the present invention utilized as an intrusion detector;

FIG. **7** is a block diagram of the information security analysis system of the present invention as an offensive tool for testing for a node attack or information hijacking; and

FIG. **8** is a typical display illustrating an object-oriented network visualization in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. **1**, there is illustrated an information security analysis system **10** including a discovery tool **12** for actively or passively monitoring a local access network (LAN) by means of a data channel **14**. Functionally, the discovery tool **12** comprises: sensor management, passive network discovery (network viewer, network topology); packet analyzer, knowledge base viewing, and alerting and reporting. In addition, the discovery tool **12** collects traffic and usage data and maps the network connectivity. Data collected by the discovery tool **12** becomes part of a knowledge base **16** stored in memory. Data is organized by major categories as follows: Address, Host, LM-Host, Domain, LM-Domain, SubNet, IP-Address, WWW, MAC-Address, NetwareHost, NetwareNetwork, NetwareStation, Alert, NetwareServer Type, Application, OS, WWW-Browser, WWW-Server, HTTP-Server, NNTP-Server, Protocol, User, POP3-User, FTP-User, SMTP-Sender, SMTP-Receiver, POP3-Password, FTP-Password, Router, and Vendor.

Data in the knowledge base **16** is made available to a data parsing tool **18** that converts the captured network data from the discovery tool **12** to a form useable by downstream programs of the system. Data accessed by the parsing tool **18** is then available to analytical engine **20** for analyzing the data captured by the discovery tool **12** and supports the merging of several data files and the development and comparison of network usage patterns. The analytical engine **20** may be implemented by software from i2 Inc. and marketed under the trademark "Analyst's Notebook". A second analytical engine **20** from the Department of Defense called PROPELLER is also available. The present invention is also capable of utilizing additional analytical engines as such engines become available. The analytical engines **20** are a dynamic set of graphic tools for capturing and displaying a variety of relational data sets in a format referred to as a "link chart". By use of the analytical engine **20**, such as "Analyst's Notebook", data collected can be exploited to characterize and document network characteristics and/or locate possible network intruders. After collecting and organizing data, the analytical engine **20** can be used to make associations between a number of different data charts to determine correlation or differentiation. Relationships between and array of data sources are then available to verify hypothesis, to correlate relationships among multiple data sets and to identify target data within a large data set. Network data needs to be analyzed in order to relate knowledge base data to session data, packet data, and alert data. These relationships assist in determining who has been talking to whom, as well as the content of the traffic for specific protocols (HTP, HTTP, NNTP, POP3, SMTP, TELNET, and IMAP). In the process of analyzing network data, a determination is made as to what IP and/or MAC addresses are common to more than one data set. Charac-

terizing the network in this way, requires taking a periodic snapshot of captured data over a time period. The average of what IP and MAC addresses exists are used to create a link chart representing traffic between each address set. This same process characterizes either a portion of a network or the entire network.

By operation of the analytical engines **20**, commonly reused resources may be determined by use of a sampling technique. A time period of interest is identified that will reveal common usage and data is captured during that period. For example, to determine the volume of E-mail traffic between 11:00 a.m. and 1:00 p.m., sampling would occur each day for several weeks until similarities in traffic source and destinations are apparent. After completion of the sampling, the analytical engines **20** can create a chart that inventories all of the IP and/or MAC addresses that have been identified in the sampling.

Several options are available for displaying the analyzed data including a 2-D display **22** and a 3-D display **24**. Each of the tools **12** and **18**, the analytical engine **20** and the displays **22** and **24** are functionally interconnected to an operator software interface for receiving instructions from an operator of the information security analysis system **10**.

The system of FIG. **1** accepts external sensor data (i.e., biometric information, billing data, SS7, PBX, paging information) in digital formats. When the external data is combined with network discovery and analysis tools there is provided a clear picture of the total communication security process. Thus, the system of the present invention combines physical security needs with electronic communication systems and IS/IT/CIO departments into a complete surveillance package.

In accordance with operator instructions, the system records and plays back selected portions of the stored database for after the-fact analysis and visualization in two or three dimensions. This is adaptable for external sensor and/or intrusion detection data.

In addition, the system of FIG. **1**, may decode FTP, HTTP and TELNET, POP3, SMTP, NNTP, and IMAP sessions in near real time and/or after the fact. The modular architecture of the present invention allows plug-in modules to be added to further enhance and expand protocol decodes to include session reconstruction. This feature permits the analysis system **10** to automatically determine the context of information traveling on an Intranet. This information is then put into nodal diagrams for Network Security personnel to determine what information needs further protection. It also can be used to answer the questions like: are illegal businesses being conducted within the Intranet; what if any harassment is taking place from an employee to another individual; where are employees spending their time on the World Wide web.

In one implementation of the information security analysis system **10**, a Pentium-based PC was utilized with a minimum of 166 MHz CPU running the WindowsNT 4.0 operating system. Further, the analysis system **10** included 64 megabyte of real RAM, a 1-gigabyte hard drive and a 17-inch monitor. Improved operation of the information security analysis system **10** is achieved by utilization of a PentiumII/300 or better with 128 megabyte of real RAM, a 4 gigabyte hard drive and a 21 inch monitor.G13

Referring to FIG. **2** there is shown a flow diagram of one application of the information security analysis system **10** of FIG. **1**. A passive data discovery engine (discovery tool **12**) is utilized to gather data regarding a network and once discovered the data is inserted into the knowledge base **16**. Specifically, the discovery tool **12** gathers data to grab small computer source and executable code nodal diagram in two and three dimensional space Collection of this data enable scaling and displaying large computer code nodal diagrams thereby permitting an analyst the flexibility to view and observe the interconnections within a large body of code for computer equipment that supports digital data communication networks. Gathering computer source and executable code by the discovery tool **12** also enables the system of the present invention to synthetically simulate small computer source and executable code program while viewing related nodal diagram in 3-D space. This enables the determination of where a malicious code might reside within a program, identify memory locations where the data resides after a program has finished execution, and use graphic vectors as templates to find specific types of code modules (that is, viruses, encryption algorithms). In addition the discovery tool **12**, collects data on intranets (that is, LAN/WAN) for simultaneous display in two-dimensions the physical and virtual network diagrams. This enables the system analysis to instantaneously display physical equipment net connection of a data communications network. By way of example, by implementing a sum and difference routine, a system analyst is able to determine when new terminals and/or configurations are added or removed from the network to include possible identification of intranet "backdoors". Collection of this data on internets enables virtual intranet diagrams thereby permitting real time analysis of how the network is being used, who is communicating with whom, determination of potential choke points and vulnerabilities, limited "trace route" reconstruction and types of worldwide web service requested.

In addition, the discovery engine gathers structure information on the network, the method of operation of the network and network users. A typical discovery engine coordinates information from multiple sensors to provide an in-depth picture of network data. In addition, the discovery engine collects data on an operating session of a network in addition to packets of meta data all created along with the knowledge base as "flat files". In addition to gathering and analyzing Ethernet LAN traffic the discovery engine may also be configured to gather and analyze data on other types of network traffic including ATM, WAN protocols, and cellular communications.

The discovery engine (discovery tool **12**) generates a knowledge base of data learned about a network and this data is stored in an appropriately named file in a stored data directory of the discovery tool **12**. The format of the flat text file from the discovery engine is now processed for further utilization by the information security analysis system **10**.

This text knowledge base flat file is processed by the data parsing tool **18** utilizing a keyword search of the knowledge base file to generate data in various categories. For example, data is organized in various categories as follows: unique user identification, host, LM-host, domain, LM-domain, SubNet, IP-address, WWW, MAC-address, NetWare host, NetWare network, NetWare station and various other available categories.

In addition to organizing the knowledge base **16** into various categories, the parsing tool may also create hashed output files.

Following parsing of the knowledge base **16** the analytical engine **20** responds to the data for preparation and converting into vector-based nodal diagrams. Typically the analytical engine **20** creates associations between a number of different charts to determine if such data charts correlate or

differentiate. Relationships between an array of data sources is utilized to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set. Based on this analysis, the information security analysis system enables the development of resources for management of a network.

The analytical engine **20** analyzes network data to relate knowledge base data to session data, packet data, and alert data as these relationships are utilized to determine who has been talking to whom as well as the content of the traffic for specific protocols.

In the process of analyzing network data received by the discovery tool **12** (discovery engine) a determination must also be made as to what communication exist in more than one data set. Characterizing the data in this way utilizes taking a periodic snapshot of captured data over a time period. Averages are then made of what relationships exist to create a link chart representing traffic between data sets.

Referring to FIG. 3 there is shown the architecture of a typical discovery tool **12** of FIG. **1** as illustrated in the application flow diagram of FIG. 2. One or more sensors are controlled by means of a specialized sensor to provide setup, collection, and transmit control. For the local Ethernet sensor an Ethernet driver sits above the NDIS layer to provide raw packets of network data. Packets of data are queued by a sensor manager **32** and then provided to all the tools in a tool suite **34**. An internal packet-processing engine **36** decodes data packets and converts the raw data to information elements that are accessible to all the tools in a tool suite **34**. In addition, a script engine **38** filters particularly interesting information and enters knowledge into the knowledge base **16**. This database is also accessible by all the tools in the tool suite **34**.

In addition to a specialized sensor, the discovery tool **12** also includes control of remote sensor **42**. The remote manager **40** queries the remote sensor, for example, a web based monitor and query tool, to be provided to all the tools in the tool suite **34**.

As illustrated in FIG. 3 the discovery tool 12 is organized as a tightly coupled sensor/processor that is based on a suite of inter operable tools. These tools provide visualization, mapping, and analysis of incoming data and processed knowledged. The sensor manager tool **80** provides configuration and control of the sensors within the discovery tool **12** that allows data to be collected (local or remote sensors) without being transmitted to the discovery tool. Various aspects of the sensor manager tool **80** include providing a view of sensors sorted at a top level according to the host, collection of all sensor data within a category, enables transmission of data from sensors to the discovery tool, again by selected category, enables communication from a remote sensor to the discovery tool, adds a new (remote) host and associated sensors to the sensor management tool control.

The network viewer tool **82** provides auto-discovery, auto-layout, and automatic visualization of network nodes and links. Nodes are sources of computer traffic, and include servers, hosts and clients. Links are representations of end to end traffic, and may transfer to higher level network elements (such as routers). The network viewer tool **82** reads packet information and provides a physical picture of one or more logical networks. The logical picture displays nodes and links information and provides a physical picture of one or more logical networks. The logical picture displays node and link information aggregated for multiple packets. Inasmuch as network traffic (nodes and links) exists at many instances of the OSI network model (data link, etc.), effective visualization occurs by examining the source network at many different layers. In one embodiment of the network viewer tool **82** circles on a graph window represents nodes and lines represent communication links. As the discovery tool **12** automatically discovers more nodes, the count for each network appears on the graph window along with a network label. As the node representation is tree-based, the count is an aggregate of all nodes below the reference node. Information that is relevant to a node from the knowledge base **16** will be displayed in the window of the object viewer tool **84**.

The object viewer tool **84** is integrated with the network viewer tool **82**, the topology display tool **90**, and a query consult tool **94**. The object viewer tool **84** actuates the display of information regarding all transitive relations (that are not address-based) that can be made regarding an object. For example, if an IP-address is associated with the user, and a user is associated with a host address, then these will all be a part of the object viewer tool display. However, if the host address is further associated with another IP-address, this transitive association is not displayed because of the confusion that may result in interpreting relations. With nodes being objects and links being relations, the object viewer tool **84** creates a list of objects displayed in a sort by class.

Analysis of data packets and data packet structure is provided by activation of the packet viewer tool **86**. This provides the structure of or information within network packets and also helps to discern and understand new, unusual and/or proprietary protocols. When the packet viewer tool **86** is activated, a packet filter (not shown) is initially set to allow all updated packets to be captured. When a user is interested in certain packet types, then the packet viewer tool **86** allows the user to select certain subsets of packets via a packet filter setup dialog. Although the packet viewer tool **86** is useful for protocol debugging and development, the functionality of this tool also is useful to browse for new packet types.

Turning next to the knowledge browser tool **88**, this tool is a visual interface for the knowledge base **16** and provides a tree-based approach to browsing objects in classes within the knowledge base, and in addition provides linkage information for tracing items and information passively discovered on the network by the discovery tool. The knowledge browser tool **88** enables acquisition, organization, and the categorization of network information, of tasks that require both automation for simplicity and customization for user accessibility.

Loosely, a class browsed by the knowledge browser tool **88** is an item in the knowledge base **16** containing categorized information, and can contain subclasses, objects, or both. Examples of classes are IP-ADDR, MAC-ADDR, and SMTP-sender An object, as considered in the context of the present invention, is a member of a class, and is an item in the knowledge base **16** having network-specific information.

The discovery tool **12** includes the script engine **38** (running as a separate thread) for processing information elements within received protocols to gather intelligence about objects within a network. Standard object types include users, hosts, domains, applications and addresses, however, and ontology specification allows new objects to be added. Using one way or two way bindings to relay information (for example, host and user), associations are made using information elements across multiple protocol/object types. Essentially, in accordance with the function of

the present invention, a network becomes a linked graph contained in multi-dimensional space, where relationships are stored as links between vectors within this space.

Next, considering the topology display tool **90**, this tool provides a compact, automatically generated view of the elements of a network identified by the discovery tool **12**. FIG. **8** shows a typical window display upon activation of the topology display tool **90**. Based on information contained within the knowledge base **16**, the topology display tool **90** shows routers, SubNets, and user nodes. Furthermore, a subset of classes within the knowledge base **16** can be overlaid on top of this view. For example, host names and vulnerabilities can be shown.

The session recorder tool **92** enables packet reassembly, TCP/IP session management, and knowledge discovery. This tool is a mechanism for observing multiple session types which cannot easily be handled at the packet level, for example: HTTP, POP3, SMTP, SNMP, TELNET, NNTP, and IMAP. By reassembling packets and looking for key aspects of information across the reassembled packets, the session recorder tool **92** provides the capability for observing and learning about application level entities on the network.

In operation, the session recorder tool **92** reassembles connection-oriented flows, or sessions. These layer-4 (e.g., TCP) and above sessions consist of multiple packets, to be reassembled and parsed to expose application-level information. Packet and cell reconstruction techniques provide the user with state information (for example, call progress and session monitoring), as well as application layer information (for example, e-mail addresses). Utilizing session search techniques within the session recorder tool **92**, combined with alert processing, capabilities (such as seeing when a certain user gets e-mail) can be flexibly constructed. In one implementation of a session recorder tool **92** there is provided viewing of the following sessions: HTTP, POP3, TELNET, FTP, SMTP, NNTP, and IMAP. During operation of the session recorder tool **92** data can be added to the knowledge base **16** as the tool detects, processes and scans sessions for various pieces of information.

The query consult tool **94** provides a text-based interface to the knowledge base **16**. By utilization of the query consult tool **94**, a user is able to determine if the knowledge base **16** contains an object (for example, individual IP address) or determine the set of objects belonging to a class of the knowledge base **16** (for example, IP-ADDR). In one implementation of the query consult tool **94**, the knowledge base **16** was queried for top level class names, objects belonging to a given class and specific class objects.

In addition to the tool suite **34**, the discovery tool **12** includes a knowledge base parsing tool set **96** as shown in FIG. **3**. Following discovery of the data from the network under analysis, the data is then appropriately formatted for use by the analytical engine **20**. The knowledge base parsing tool set **96** functions to take the collected data and put it into the appropriate format for use by the analytical engine **20**. Individual tools in the knowledge base parsing tool set **96** are available to parse data from the knowledge base **16** and extract information from saved log files and reassembled session files. The knowledge base parsing tool set **96** comprises eight tools: KB parsing, E-mail extraction, session joining, web extraction, graphics extraction, KB summing, file manipulation, and column splitting.

The network discovery tool generates the knowledge base **16** of data assembled about a network. This data is stored in a flat text file and saved for reuse by the discovery tool **12** for display of a network. The format of the text, however, is not useful for follow on processing. The KB parsing tool, parses the data to be output for display in a columnar file, to be imported to a database, or to the analytical engines **20**. In addition, the KB parsing tool is utilized as a key word search to generate data in various categories.

As explained, the session recorder tool **92** is a mechanism for observing multiple session types and generates files containing reassembled session data. The number of files created during a single data collection may, for example, exceed 10,000. The E-mail extraction tool of a knowledge base tool in the tool set **96** provides for organizing POP3 and SMTP files into summary descriptions. The summary descriptions are then imported to a database or to the analytical engine **20**. The E-mail extraction tool contains a key word search mechanism as well as other types of data parsing.

As mentioned, the discovery tool **12** generates a knowledge base of flat file data collected about a network. The web extraction tool of a knowledge base tool set **96** facilitates the parsing and formatting of data from HTML flat files that are then imported to a database or to the analytical engines **20**. The web extraction tool contains a tag (similar to a key word) search mechanism as well as other types of data processing algorithms.

The graphics extraction tool of the knowledge base tool set **96** provides for reassembling image files from a recorded format. The display of the session recorder tool **92** provides for the recording of HTTP sessions. These session files contain a header describing the session and the data associated with the session. When a JPG or GIF image is downloaded, the data is reassembled in the session. However, this data is not displayable in the recorded format. The graphic extraction tool converts the reassembled HTTP session file containing JPG and GIF data and creates a new log file containing the names and images.

Data stored in a flat text file by operation of the discovery tool **12** is utilized by the KB summation tool of the knowledge base tool set **96** to create a statistical matrix of the data contained in packet and session logs. For example, the instance of a protocol may be used as the Y access and the source IP address may be used as the X access. After selection of the packet or session log has been made, the KB summation tool screens the appropriate log file and displays available access criteria to create a graph. In the analysis of a typical network, a large number of files will be generated. The file manipulation tool of the knowledge base tool set **96** provides an interface to reduce the volume of generated files that must be sorted through. It enables files to be deleted or moved based on the file size, type, or contents for purposes of enhancing subsequent processing. Generated files are processed according to a chosen criteria for all files in a group.

Recorded sessions of the discovery tool **12** are occasionally truncated and restored as a new session. These truncated sessions are preferably reassembled before viewing. The session joining tool of the knowledge base tool set **96** connects all truncated sessions into completed transactions.

Also included in the knowledge base tool kit **96** is a split data column tool. This tool is used to remove unwanted columns of data from log files.

Referring to FIG. **4**, there is shown a structuring of the information in the knowledge base **16**. The definition and structure of the knowledge is taken into consideration to improve the ability to understand the knowledge prior to processing network information. FIG. **4** is an organizational

chart of categories of information assembled in the knowledge base by the discovery tool **12**. The knowledge base is an object-oriented relational entity that is stored as a flat text file and is information collected from packets on the data channel **14**.

Referring to FIG. **5**, there is illustrated a block diagram of the 3-D display **24** including a visualization pre-processor **100** receiving raw ASCII data from the analytical engine **20**. Also input to the visualization pre-processor **100** through a software link **108** is a visualization setup file **102**, a linking information file **104** and a field key file **106**. Following processing of the data from the analytical engine **20**, the visualization pre-processor **100** transfers the processed data to a 3-D rendering engine **110**. The rendering engine **110**, a commercial off the shelf software package, formats the information in accordance with user instructions from an input device **114** and arranges the information for input to a display **112**.

Through the use of head mounted display technology and a six degree of freedom tracking system receiving data from the preprocessor **108**, a user will experience full viewing immersion within the network identified with the data in the knowledge base **16**. This technology provides the user with the further ability to interact and negotiate with the network data display, as opposed to a traditional flat display.

Referring again to FIG. **1**, the 3-D display **24** adds a third dimension to any of the data collected by the discovery tool **12** to view, animate, and analyze complex nodal diagrams in 3-D space. This is required because the raw data file only contains two dimensions. If the data from the analytical engines outputted three or more dimensions, the 3-D display would not be required to add a third dimension. The addition of a third vector permits the simultaneous viewing of large complex diagrams on interconnected planes in accordance with user instructions from the input device **94**. The display of FIG. **5** permits an analyst to rotate the diagram on any axis thereby viewing relationships that otherwise become obscure viewed on two-dimensional planes.

Referring to FIG. **6** there is shown a representative utilization of the analysis system **10** of the present invention as illustrated in FIG. **1**. The analysis system **10** is operated on a terminal **46** as part of a network including terminals **48**, **50** and **52**. The network including the terminals **46**, **48**, **50** and **52** is interconnected through a firewall **54**. The firewall **54** interfaces with a network **56** that includes a network analyzer **58**. The analyzer **58** analyzes inbound traffic to the terminals and also monitors for "meta data" associated with an intruder inbound to the network. Typically, the analyzer **58** establishes specific meta data associated with an inbound intrusion. As illustrated in FIG. **6**, the network **56** is coupled to a gateway **60** and a terminal **62** representing a remote intruder to, for example, the terminal **48** as a target.

In the present example it will be assumed that the remote intruder on terminal **60** is attempting to send an E-Mail to the target terminal **48** behind the firewall **54**. The analysis system **10** of the present invention running on the terminal **46**, monitors through the discovery tool **12** the Ethernet level inbound e-Mail The analysis system **10** records inbound e-mail traffic as part of the knowledge base **16** such as post office protocol version 3 (POP3) and the simple mail transfer protocol (SMTP). In addition, the analysis system **10** examines meta data associated with inbound E-Mail and further examines SMTP/POP3 packets inbound to the target terminal **48**. Identified SMTP/POPS packets inbound for the target terminal **48** are passed to the analytical engine **20** for analysis. As previously explained, the analytical engine **20** imports the meta data passed by the discovery tool **12** for analysis and display.

Referring to FIG. **7** there is shown a utilization of the analysis system **10** of the present invention in an environment of a multi-node network. As illustrated, the network includes nodes **64**, **66** and **68**. Interconnected to the node **68** is a terminal **70** running the analysis system **10** as illustrated in FIG. **1**. Also interconnected into the node **68** is a network analyzer **72**. Each of the nodes **64**, **66** and **68** interconnect to a firewall **74**. The firewall **74** in turn is behind an additional firewall **76** that interconnects to a wide area network (not shown).

In this example the analysis system **10** as running on the terminal **70** monitors the level of intranet traffic and records packets of data from each of the terminals of the various nodes. For a terminal under attack, such as terminal **64***a*, the analysis system establishes a target source packet structure and by means of the analytical engine **20** of the present invention could be modified to shut down a target under attack.

It should be understood that FIGS. **6** and **7** are only two examples of utilization of the analysis system **10**. Additional uses of the information security analysis system **10** include offensive and defensive information viewing, context nodal visualization of simultaneous E-mails, FTP and TELNET sessions, graphical playback of filtered nodal traffic, analyzing of computer source and executable code, passively and dynamically discovery of local area network or wide area network physical and virtual connectivity, detection intrusion both internal and external to a local area network or wide area network such as described with reference to FIG. **6**, automatically alert and take corrective action when a network is under attack, FIG. **7**, and detection of computer viruses.

While the invention has been described in connection with a preferred embodiment, it is not intended to limit the scope of the invention to the particular form set forth, but, on the contrary, it is intended to cover alternatives, modifications, equivalents as may be included within the spirit and scope of the invention as defined in the appended claims.

What is claimed is:

1. A method for templating and viewing virus computer code for data communications networks, comprising:

gathering from a host computer information on a bit stream of computer code prior to execution by the host computer;

generating a knowledge base of the bit stream of the computer code gathered from the host computer;

parsing the information in the knowledge base to generate data into structured files having a readable format;

analyzing the data in the structured files to derive a genetic structure and examine the functionality of suspect computer code;

comparing a plurality of genetic structures to determine the presence of a computer virus; and

visualizing the structured files to display in a user interactive graphical functional mode functionality of suspect computer code to identify the presence of a computer virus prior to execution in the host computer.

2. The method for templating and viewing a virus computer code as set forth in claim **1** wherein analyzing the data comprises determining internal and external intrusion attempts.

3. The method for templating and viewing a virus computer code as set forth in claim **1** wherein comparing a

plurality of genetics structures comprises determining when the derived genetic structure resides in the suspect computer code to determine the presence of a computer virus.

4. The method for templating and viewing a virus computer code as set forth in claim 1 wherein analyzing the data comprises documenting and organizing the computer code in a functional relationship.

5. The method for templating and viewing a virus computer code as set forth in claim 1 wherein gathering information comprises passively collecting information on the bit stream of the computer code.

6. The method for templating and viewing a virus computer code as set forth in claim 1 wherein analyzing the data comprises analyzing attachments to an E-mail message.

7. The method for templating and viewing a virus computer code as set forth in claim 1, wherein comparing a plurality of genetic structures comprises determining the degree of functional alteration.

8. A method for templating and viewing virus computer code for data communications networks, comprising:

gathering from a host computer information on a bit stream of computer code prior to execution by the host computer;

generating a knowledge base of the bit stream of the computer code gathered from the host computer;

parsing the information in the knowledge base to generate data into structured files having a readable format;

analyzing the data in the structured files to derive a genetic structure and examine the functionality of suspect computer code;

comparing a plurality of genetic structures to determine the presence of a computer virus; and

displaying in a user interactive graphical functional mode the structured files to identify the presence of a computer virus prior to execution in the host computer.

9. The method for templating and viewing a virus computer code as set forth in claim 8 wherein comparing a plurality of genetic structures comprises determining when the derived genetic structure resides in the suspect computer code to determine the presence of a computer virus.

10. The method for templating and viewing a virus computer code as set forth in claim 8 wherein analyzing the data comprises documenting and organizing the computer code in a functional relationship.

11. The method for templating and viewing a virus computer code as set forth in claim 8 wherein gathering information comprises passively collecting information on the bit stream of the computer code.

12. The method for templating and viewing a virus computer code as set forth in claim 8 wherein analyzing the data comprises analyzing attachments to an E-mail message.

13. The method for templating and viewing a virus computer code as set forth in claim 8, wherein comparing a plurality of genetic structures comprises determining the degree of functional alteration.

14. A method for templating and viewing virus computer code for data communications networks, comprising:

gathering from a host computer information on a bit stream of computer code prior to execution by the host computer;

generating a knowledge base of the bit stream of the computer code gathered from the host computer;

analyzing the data in the knowledge base to derive a genetic structure and examine the functionality of suspect computer code;

comparing a plurality of genetic structures to determine the presence of a computer virus; and

visualizing the analyzed data to display in a user interactive graphical functional mode functionality of suspect computer code to identify the presence of a computer virus prior to execution in the host computer.

15. The method for templating and viewing a virus computer code as set forth in claim 14 further comprising functionally interconnecting an operator software interface to the gathering of information, generating a knowledge base of the operator software, and analyzing the data to receive instructions from an operator.

16. The method for templating and viewing a virus computer code as set forth in claim 15 further comprising formatting the analyzed data in accordance with user instructions for visualization to identify the presence of a computer virus.

17. The method for templating and viewing a virus computer code as set forth in claim 14, wherein comparing a plurality of genetic structures comprises determining the degree of functional alteration.

18. A method for templating and viewing virus computer code for data communications networks, comprising:

generating a knowledge base of a bit stream of a computer code;

parsing the information in the knowledge base to generate data into structured files having a readable format;

analyzing the data in the structured files to derive a genetic structure of suspect computer code to determine the presence of a computer virus;

displaying in a graphical functional mode the analyzed data to determine the presence of a computer virus prior to execution in a host computer; and

rotating the analyzed data on an axis on two or more separate but connected visual planes.

19. A method for templating and viewing virus computer code for data communications networks, comprising:

generating a knowledge base of a bit stream of a computer code;

parsing the information in the knowledge base to generate data into structured files having a readable format;

analyzing the data in the structured files to derive a genetic structure of suspect computer code to determine the presence of a computer virus;

displaying in a graphical functional mode the analyzed data to determine the presence of a computer virus prior to execution in a host computer; and

appending user definable symbols for enhancing an understanding by an operator or analyst.

20. A method for templating and viewing virus computer code for data communications networks comprising a plurality of nodes, comprising:

generating a knowledge base of a bit stream of a computer code;

parsing the information in the knowledge base to generate data into structured files having a readable format;

contracting several nodes of a data communications network into a single interconnecting common node for analysis to determine the presence of a computer virus

analyzing the data in the structured files to derive a genetic structure of suspect computer code to determine the presence of a computer virus; and

displaying in a graphical functional mode the analyzed data to determine the presence of a computer virus prior to execution in a host computer.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
Certificate

Patent No. 6,253,337 B1 Patented: June 26, 2001

On petition requesting issuance of a certificate for correction of inventorship pursuant to 35 U.S.C. 256, it has been found that the above identified patent, through error and without any deceptive intent, improperly sets forth the inventorship.

Accordingly, it is hereby certified that the correct inventorship of this patent is: Michael P. Maloney, Severna Park, MD; John M. Suit, Pasadena, MD; Christopher J. Scott, Mt. Airy, MD; Richard R. Rubel, Glen Burnie, MD; and Francis M. Woodus, Owing Mills, MD.

Signed and Sealed this Eleventh Day of February 2003.

ROBERT W. BEAUSOLIEL, JR.
Supervisory Patent Examiner
Art Unit 2184

#4/a

RECEIVED
CENTRAL FAX CENTER
DEC 0 3 2003

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICIAL

In re: *Jaffe et al.*

U.S. Serial No.: 09/626,044

For: INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES

Filed: 07/27/2000

Attorney Docket No.: 6468/78445

Group Art Unit: 2131

Examiner: Hosuk Song

I hereby certify that this paper is being sent by facsimile to (703) 872-9306 as the USPTO Central Facsimile Number and Directed to Mail Stop Non-Fee Amendment, Hon. Commissioner of Patents & Trademarks Alexandria, VA 22313-1450 on this date:

12/03/2003
Date

Signature
Corri Feuerstein
Printed Name

AMENDMENT A

Commissioner of Patents & Trademarks
Mail Stop Non-Fee Amendment
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Reply and Amendment is in response to the non-final Official Action mailed March 14, 2003. Continued prosecution and reconsideration of the above-identified application is respectfully requested in view of the amendments below and the discussion that follows.

In the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Please cancel claims 1-8 and add new claims 9-14 as follows.

9. (new) A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said image;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

10. (new) The method of claim 9, wherein said memory form a part of a digital camera.

11. (new) The method of claim 9 wherein said at least one parameter comprises a

PAGE 4/7 * RCVD AT 12/3/2003 5:35:47 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:312 655 1501 * DURATION (mm-ss):01-24

random number.

12. (new) The method of claim 9, further comprising the step of appending at least one additional parameter to said data file in said memory, said at least one additional parameter being generally representative of a condition under which said data stream was generated.

13. (new) The method of claim 12, wherein said at least one additional parameter is selected from a group consisting of: GPS coordinates, zoom settings, AutoFocus status, focus quality sampling, roll, pitch and yaw values, compass headings, flash status, CamID, Seq, and a Security Value.

14. (new) The method of claim 9 wherein said data stream is a digital sample of an environment.

PAGE 5/7 * RCVD AT 12/3/2003 5:35:47 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:312 655 1501 * DURATION (mm-ss):01-24

Remarks:

It is respectfully submitted that new claims 9-14 are not subject to rejection over U.S. Patent No. 5,764,770 to Schipper et al. (the "Schipper patent") for a number of reasons, including those set forth hereinafter. For example, the Schipper patent does not teach or suggest structure or method steps corresponding to the feature of new claims 9-14 that states,

> "utilizing a sensor, which is *tightly coupled to said memory*, to generate at least one internal and unique parameter " (emphasis added).

Exemplary structure or method steps corresponding to this claim feature is shown in Fig. 2A of the subject application, which illustrates a processor 157 which is "tightly coupled" to a memory. In one exemplary embodiment of the present invention, the processor 157 generates a unique random string that is used for image authentification purposes. Because the processor is "tightly coupled" to the memory, it will be virtually impossible for a user to supply false information to the memory by breaking the conductive trace or lead between the memory and the processor. This means, for example, that there is no possibility for altering the image before the authentification information is generated.

The Schipper patent teaches no such "tight coupling." In direct contrast to this, the relevant portion of the Schipper patent cited by the Examiner in the Office Action relating to this issue (column 15, lines 30-45 and 59-67) teach that authentification is accomplished by comparison of *position* information, which must originate from devices *external* to the camera, such as satellites in orbit around the earth. The Schipper system can be fooled by supplying false position signals to the recording device, which is not the case with the claimed invention. For this reason alone, new claims 9-14 should be found to be allowable over the Schipper patent.

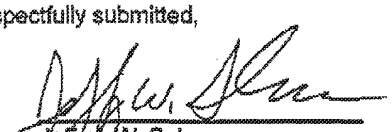
Moreover, the Schipper device is unreliable from the perspective that it is rendered inoperative to the extent that the GPS satellites go down. The present invention is not subject to such limitations. Rather, it should always operate, irrespective of the presence or absence signals external to the device, so long as it is supplied with electric power.

It is respectfully submitted that new claims 9-14 are in condition for allowance. A formal notice to that effect is earnestly solicited. If the Examiner is of the opinion that a telephone

PAGE 6/7 * RCVD AT 12/3/2003 5:35:47 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:312 655 1501 * DURATION (mm-ss):01-24

conference would expedite the prosecution of the above-captioned application, then he is respectfully requested to contact the undersigned attorney at his convenience.

Respectfully submitted,

By: 

Jeffrey W. Salmon
Reg. No. 37,435

Dated: December 3, 2003

WELSH & KATZ, LTD.
120 South Riverside Plaza, 22nd Floor
Chicago, Illinois 60606
(312) 655-1500 (telephone)
(312) 655-1501 (facsimile)

PAGE 7/7 * RCVD AT 12/3/2003 5:35:47 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:312 655 1501 * DURATION (mm-ss):01-24

120 South Riverside Plaza
22nd Floor
Chicago, Illinois 60606
Phone: (312) 655-1500
Fax: (312) 655-1501

WELSH & KATZ, LTD.

RECEIVED
CENTRAL FAX CENTER
DEC 0 3 2003
OFFICIAL

Fax

To: USPTO Mail Stop Non Fee Amendment **From:** Jeffrey W. Salmon, Esq.
Examiner Hosuk Song

Fax: (703) 872-9306 **Pages:** 7 with cover page

Phone: **Date:** 12/3/2003

Re: S.N. 09/626,044 **CC:**

☐ **Urgent** ☐ **For Review** ☐ **Please Comment** ☐ **Please Reply** ☐ **Please Recycle**

IF YOU DO NOT RECEIVE ALL PAGES OR ARE HAVING TROUBLE, PLEASE CALL IMMEDIATELY (312) 655-1500 AND ASK FOR Corri Feuerstein.

******** CONFIDENTIALITY NOTE ********

The documents accompanying this facsimile transmission contain information which may be confidential or privileged and exempt from disclosure under applicable law. The information is intended to be for the use of the individual or entity named on this transmission sheet. If you are not the intended recipient, be aware that any disclosure, copying distribution or use of the contents of this information is without authorization and is prohibited. If you have received this facsimile in error, please notify us by collect telephone immediately so that we can arrange for the retrieval of the original documents at no cost to you.

CERTIFICATE OF TRANSMISSION BY FACSIMILE (37 CFR 1.8) Applicant(s): Jaffe et al.			Docket No. 6468/78445
Serial No. 09/626,044	Filing Date 07/27/2000	Examiner Hosuk Song	Group Art Unit 2131

Invention: **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**

RECEIVED
CENTRAL FAX CENTER
DEC 0 3 2003
OFFICIAL

I hereby certify that this **Amendment A**
(Identify type of correspondence)
is being facsimile transmitted to the United States Patent and Trademark Office (Fax. No. **(703) 872-9306**

on **12/03/2003**
(Date)

Corri Feuerstein
(Typed or Printed Name of Person Signing Certificate)

(Signature)

Note: Each paper must have its own certificate of mailing.

PAGE 2/7 * RCVD AT 12/3/2003 5:35:47 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:312 655 1501 * DURATION (mm-ss):01-24

281

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/626,044	07/27/2000	Jonathan E. Jaffe	6468/78445	9426

7590 02/24/2004

Welsh & Katz
120 south Riverside Plaza
22nd Floor
Chicago, IL 60606

EXAMINER	
SONG, HOSUK	

ART UNIT	PAPER NUMBER
2135	5

DATE MAILED: 02/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)	
	09/626,044	JAFFE ET AL.	
	Examiner	Art Unit	
	Hosuk Song	2135	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2000* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-14* is/are pending in the application.

4a) Of the above claim(s) *1-8* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

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

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

ADOBE – Exhibit 1002, page 282
JAFFE-ADOBE000316

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 9-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schipper et al.(US 5,764,770) in view of Maloney et al(US 6,253,337).

Claim 9: Schipper disclose storing a data stream in a data file in a memory in (col.7,lines 62-67 and col.8,lines 1-15). Schipper disclose utilizing a signature protocol to generate a first signature based on data stream and at least one paramemeter, first signature being generated without altering data stream and being appended to data file in memory in (col.8,lines 34-49). Schipper discloses generating a second signature based on image and comparing first and second signature in (col.15,lines 30-45). Schipper discloses notifying the user whether data is valid/invalid in (col.15,lines 39-44). Schipper does not specifically discloses sensor tightly coupled to the memory. Maloney's patent discloses security processor where sensor is tightly coupled to the memory in (fig.3 and col.7,lines 40-47). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a sensor tightly coupled to the memory as taught in Maloney with data authentication device disclosed in Schipper in order to prevent unauthorized user from entering or breaking and supplying false information to memory and the processor thus data can be properly authenticated without fear of tampering.

Claim 10: Schipper disclose circuit and memory form a part of a digital camera in (fig.7 and col.59-67).

Claim 11: Neither Schipper nor Maloney specifically discloses parameter comprising a random number. Examiner takes Official notice that using a random number as parameter is well known in the art. One of ordinary skill in the art would have been motivated to use random number because random number prevent a potential thief from performing any analysis on signals captured from the remote device that would lead to an accurate prediction of a valid subsequent command signals.

Claim 12: Schipper discloses step of appending at least one additional parameter to data file in memory and at least one additional parameter being generally representative of a condition under which data stream was generated in (col.14,lines 53-65 and col.16,lines 1-28).

Claim 13: Schipper disclose GPS coordinate in (fig.1,6).

Claim 14: Schipper disclose data stream is a digital sample of an environment in (col.7,lines 63-67 and col.8,lines 2-15).

Response to Amendment

2. Applicant has cancelled claims 1-8 and added new claims 9-14. Applicant's amendment necessitated the new grounds of rejection. New grounds of rejections are presented above.

Conclusion

3. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hosuk Song whose telephone number is 703-305-0042. The examiner can normally be reached on Tue-Fri from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HS

KIM VU
SUPERVISORY PATENT EXAMINER

O I P E
MAR 1 1 2004
JC42
PATENT & TRADEMARK OFFICE

RCE
2135
#16

PTO/SB/30 (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	09/626,044
Filing Date	07/27/2000
First Named Inventor	Jaffe, et al.
Art Unit	2135
Examiner Name	Hosuk Song
Attorney Docket Number	6468/78445

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.
   i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
   ii. ☐ Other _____

RECEIVED
MAR 1 6 2004
Technology Center 2100

b. ☒ Enclosed
   i. ☒ Amendment/Reply
   ii. ☐ Affidavit(s)/Declaration(s)
   iii. ☐ Information Disclosure Statement (IDS)
   iv. ☐ Other _____

2. Miscellaneous
a. ☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)
b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
a. ☒ The Director is hereby authorized to charge the following fees, or credit any overpayments, to Deposit Account No. 23-0920
   i. ☐ RCE fee required under 37 CFR 1.17(e)
   ii. ☐ Extension of time fee (37 CFR 1.136 and 1.17)
   iii. ☐ Other _____

03/12/2004 MGEBREM1 00000047 09626044
01 FC:2801 385.00 OP

b. ☒ Check in the amount of $ 385.00 enclosed
c. ☐ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Name (Print / Type)	Jeffrey W. Salmon	*Registration No. (Attorney / Agent)*	37,435
Signature	3/8/04	*Date*	March 8, 2004

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent andTrademark Office on the date shown below.

Name (Print / Type)	Maura Halvey		
Signature		*Date*	March 8, 2004

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing the burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop RCE,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.

O I P E JC42
MAR 1 1 2004
PATENT & TRADEMARK OFFICE

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
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.

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) $385.00

Complete if Known

Application Number	09/626,044
Filing Date	07/27/2000
First Named Inventor	Jaffe, et al.
Examiner Name	Hosuk Song
Art Unit	2135
Attorney Docket No.	6468/78445

RECEIVED
MAR 1 6 2004
Technology Center 2100

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☐ Deposit Account:

Deposit Account Number: 23-0920

Deposit Account Name: Welsh & Katz, Ltd.

The Director is authorized to: *(check all that apply)*

☐ Charge fee(s) indicated below ☐ Credit any overpayments

☒ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES FOR UTILITY AND

	Extra Claims		Fee from below	Fee Paid
Total Claims	-20** =	0	X =	0.00
Independent Claims	-3** =	0	X =	0.00
Multiple Dependent			=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) $0.00

***or number previously paid, if greater; For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR § 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Statement	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	385.00
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($) $385.00

SUBMITTED BY

Complete *(if applicable)*

Name (Print/Type)	Jeffrey W. Saimon	Registration No. (Attorney/Agent)	37,435	Telephone	(312) 655-1500
Signature				Date	March 8, 2004

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

O I P E
MAR 1 1 2004
JC42
PATENT & TRADEMARK OFFICE

COPY

PTO/SB/30 (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	09/626,044
Filing Date	07/27/2000
First Named Inventor	Jaffe, et al.
Art Unit	2135
Examiner Name	Hosuk Song
Attorney Docket Number	6468/78445

RECEIVED
MAR 1 6 2004
Technology Center 2100

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.
   i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
   ii. ☐ Other _____

b. ☒ Enclosed
   i. ☒ Amendment/Reply
   ii. ☐ Affidavit(s)/Declaration(s)
   iii. ☐ Information Disclosure Statement (IDS)
   iv. ☐ Other _____

2. Miscellaneous
a. ☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)
b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
a. ☒ The Director is hereby authorized to charge the following fees, or credit any overpayments, to Deposit Account No. 23-0920
   i. ☐ RCE fee required under 37 CFR 1.17(e)
   ii. ☐ Extension of time fee (37 CFR 1.136 and 1.17)
   iii. ☐ Other _____
b. ☒ Check in the amount of $ 385.00 enclosed
c. ☐ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Name (Print / Type)	Jeffrey W. Salmon	Registration No. (Attorney / Agent)	37,435
Signature	3/8/04	Date	March 8, 2004

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent andTrademark Office on the date shown below.

Name (Print / Type)	Maura Halvey		
Signature		Date	March 8, 2004

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing the burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop RCE,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.

#7/B



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: *Jaffe et al.*	Group Art Unit: 2135
U.S. Serial No.: 09/626,044	Examiner: Hosuk Song
For: INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES	I hereby certify that this paper is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner of Patents & Trademarks Alexandria, Mail Stop RCE, P.O. Box 1450, VA 22313-1450 on this date:
Filed: 07/27/2000	March 8, 2004 Date
Attorney Docket No.: 6468/78445	Maura Halvey Printed Name

PRELIMINARY AMENDMENT

RECEIVED
MAR 1 6 2004
Technology Center 2100

Commissioner of Patents & Trademarks
Mail Stop RCE
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Reply and Amendment, which is being filed with an RCE request, is in response to the final Official Action mailed February 24, 2004. Continued prosecution and reconsideration of the above-identified application is respectfully requested in view of the amendments below and the discussion that follows.

In the Claims:

1

9. (currently amended) A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

B1 utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said image;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

2 1

10. (previously presented) The method of claim ~~9~~, wherein said memory form

34

B

a part of a digital camera.

3 1
~~11.~~ (previously presented) The method of claim ~~9~~ wherein said at least one parameter comprises a random number.

4 1
~~12.~~ (previously presented) The method of claim ~~9~~, further comprising the step of appending at least one additional parameter to said data file in said memory, said at least one additional parameter being generally representative of a condition under which said data stream was generated.

B1

5 4
~~13.~~ (previously presented) The method of claim ~~12~~, wherein said at least one additional parameter is selected from a group consisting of: GPS coordinates, zoom settings, AutoFocus status, focus quality sampling, roll, pitch and yaw values, compass headings, flash status, CamID, Seq, and a Security Value.

6 1
~~14.~~ (previously presented) The method of claim ~~9~~ wherein said data stream is a digital sample of an environment.

37

B

Remarks:

It is respectfully submitted that the amended claims are allowable over the prior art of record for a number of reasons, including the following. First, no prior art reference teaches or suggests the feature of the amended claims, which states,

> "utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter."

Exemplary support for this claim feature is disclosed, for example, at page 5, lines 22-24, which state, to "ensure authentification, additional inputs 7 other than the sensor set 4 are not accessible to the user without detection as shown in Fig. 2." Thus, in accordance with the present invention, the claimed "tight coupling" requires that the connections between the sensor and the memory not be physically accessible to a user.

The Maloney patent cited by the Examiner in the last Office Action does not teach or suggest the "tight coupling" claimed in the amended claims. While column 7, lines 40-45 of the Maloney patent do refer to a "tightly coupled sensor/processor," the patent characterizes that as a "suite of inter operable tools." There is no disclosure in the Maloney patent that physical access to the "suite of inter operable tools" is prevented. On the contrary, column 7, line 46 states that the sensors can be "local or remote." If the sensors are, in fact, "remote" from the processor, then it would be impossible to prevent physical access to the interconnections between the remote sensor and the local processor. For this reason alone, the amended claims are believed to be allowable over the prior art of record.

Second, the Maloney patent does not teach or the following feature of the amended claims, which states,

ADOBE – Exhibit 1002, page 292
JAFFE-ADOBE000326

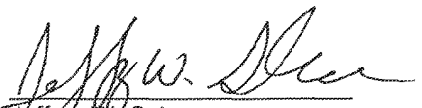
"monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity is compromised, then also providing an indication of said compromised integrity;"

Exemplary disclosure corresponding to this claim feature is shown, for example, in Figure 4A, step 59, which is a flow chart decision block in which it is determined whether internal security has been compromised. This means that, for example, a signal is generated if the device that prevents physical access to the interconnections between the sensor set and memory is broken.

No prior art reference of record, including the Maloney patent, contain any disclosure of this subject matter. For this additional reason, the amended claims are believed to be allowable over the prior art of record.

It is respectfully submitted that the amended claims are in condition for allowance, and a formal notice to that effect is respectfully solicited. Should the Examiner be of the opinion that a telephone conference would expedite the prosecution of this application, then he is requested to contact the undersigned attorney at his convenience.

Respectfully submitted,

By: 

Jeffrey W. Salmon
Reg. No. 37,435

Dated: March 8, 2004
WELSH & KATZ, LTD.
120 South Riverside Plaza, 22nd Floor
Chicago, Illinois 60606
(312) 655-1500 (telephone)
(312) 655-1501 (facsimile)

ADOBE – Exhibit 1002, page 293
JAFFE-ADOBE000327

PORTAL
THE ACM DIGITAL LIBRARY

> home > about > feedback > login

US Patent & Trademark Office

Try the *new* Portal design
Give us your opinion after using it.

Citation

ACM Transactions on Internet Technology (TOIT) >archive
Volume 3 , Issue 3 (August 2003) >toc

Location management for mobile commerce applications in wireless Internet environment

Author
Upkar Varshney Georgia State University, Atlanta, GA

Publisher
ACM Press New York, NY, USA

Pages: 236 - 255 Periodical-Issue-Article
Year of Publication: 2003
ISSN:1533-5399

http://doi.acm.org/10.1145/857166.857169 (Use this link to Bookmark this page)

> full text > abstract > references > index terms > peer to peer

> Discuss > Similar > Review this Article Save to Binder

> BibTex Format

FULL TEXT: Access Rules

pdf 630 KB

ABSTRACT

With recent advances in devices, middleware, applications and networking infrastructure, the wireless Internet is becoming a reality. We believe that some of the major drivers of the wireless Internet will be emerging mobile applications such as mobile commerce. Although many of these are futuristic, some applications including user-and location-specific mobile advertising, location-based services, and mobile financial services are beginning to be commercialized. Mobile commerce applications present several interesting and complex challenges including location management of products, services, devices, and people. Further, these applications have fairly diverse requirements from the underlying wireless infrastructure in terms of location accuracy, response time, multicast support, transaction frequency and duration, and dependability. Therefore, research is necessary to address these important and complex challenges. In this article, we present an integrated location management architecture to support the diverse location requirements of m-commerce applications. The proposed architecture is capable of

supporting a range of location accuracies, wider network coverage, wireless multicast, and infrastructure dependability for m-commerce applications. The proposed architecture can also support several emerging mobile applications. Additionally, several interesting research problems and directions in location management for wireless Internet applications are presented and discussed.

↑ REFERENCES

Note: OCR errors may be found in this Reference List extracted from the full text article. ACM has opted to expose the complete List rather than only correct and linked references.

1 Allnetdevices. 2002. Mobile Payments Set to Soar. (www.allnetdevices.com/wireless/news/2002/02/07/study_mobile.html).

2 Bisdikian, C., Christensen, J., Davis II, J., Ebling, M. R., Hunt, G., Jerome, W., Lei, H., Maes, S., and Sow, D. 2001. Enabling location-based applications, In Proceedings of the 1st ACM International Workshop on Mobile Commerce (Rome, Italy). ACM, New York, 38--42.

3 Cousins, K. and Varshney, U. 2001. Location management in B2B mobile commerce environment, In Proceedings of the 1st ACM International Workshop on Mobile Commerce (Rome, Italy, July). ACM, New York, 43--48.

4 D' hont, S. 2001. The cutting edge of RFID technology and applications for manufacturing and distribution. A Texas Instruments White Paper (available at http://www.ti.com/tiris/docs/manuals/whtPapers/manuf_dist.pdf)

5 Diercks, R. 2001. Mobile advertising: Not as bad as you think, Wireless Internet Mag. (July-August) (available at www.wirelessinternetmag.com/news/0108/0108_research_ads.htm).

6 FCC enhanced 911(www.fcc.gov/e911).

7 Djuknic, G. and Richton, R. 2001. Geolocation and assisted GPS, IEEE Comput. 34, 2, 123--125.

8 Fichtner, H., 2002. Marketing via mobile phone: Coupons conquer the mobile phone, Acquisa (available http://www.evision-ventures.de/eng/news/029.html).

9 Financial Services Technology Corporation (www.fstc.org).

10 Ghosh, K. A. and Swaminatha, T. N. 2001. Software security and privacy risks in mobile e-commerce. Commun. ACM 44, 2, 51--57.

11 Goodman, D. 2000. The wireless Internet: promises and challenges. IEEE Computer 33, 7, 36--41.

12 Koshima, H. and Hoshen, J. 2000. Personal locator services emerge. IEEE Spectrum 37, 2, 41--48.

13 Mobile Marketing Association (www.mmaglobal.com).

14 Nortel's Mobile Location Services Solution. 2002. (www.nortelnetworks.com/corporate/news/newsreleases/2002c/07_02_02_wollongong_mlc.html).

15 Paybox (www.paybox.net).

16 Rastimor, O., Korolev, V., Joshi, A., and Finin T. 2001. Agents2Go: An infrastructure for location-dependent service discovery in the mobile electronic commerce environment. In Proceedings of the 1st ACM International Workshop on Mobile Commerce (Rome, Italy, July). ACM, New York, 31--37

17 Sastry, D., Cole, A., Munson, J., and Christensen, J. 2001. An approach to providing a seamless end-user experience for location-aware applications. In Proceedings of the 1st ACM International Workshop on Mobile Commerce (Rome, Italy, July). ACM, New York, 20--25.

18 Sprint and eone Mobile Payment Network. 2002. (www.mcommercetimes.com/Services/254).

19 Tracz R. and Wrona, K. 2001. Fair electronic cash withdrawal and change return for wireless networks. In Proceedings of the 1st ACM International Workshop on Mobile Commerce (Rome, Italy, July). ACM, New York, 14--19.

20 Varshney, U. 2001. Addressing location management issues in mobile commerce, In Proceedings of IEEE Conference on Local Computer Networks (LCN-26) (Tampa, Fla., Nov.). 184--192.

21 Varshney, U. 2002. Mobile commerce: Issues, technologies, and solutions, A tutorial at ACM International Conference on Mobile Computing and Networking (Mobicom) (Atlanta, Ga., Sept.) ACM, New York.

22 Varshney, U. and Malloy, A. 2001. An integrated approach for improving the dependability of the emerging wireless networks. In Proceedings of IEEE International Conference on Global Communications (Globecom) (San Antonio, Tex., Nov.) IEEE Computer Society Press, Los Alamitos, Calif., 3693--3697.

23 Varshney, U. and Vetter, R. 2002. Mobile commerce: Applications, frameworks, and networking support. ACM/Kluwer J. Mob. Netw. Appl. (MONET) 7, 3, 185--198.

24 Varshney, U., Vetter, R., and Kalakota, R. 2000. Mobile commerce: A new frontier. IEEE Computer 33, 10, 32--38.

25 Vodafone Mobile Payment System. 2002. (www.pcmag.co.uk/News/1128273).

INDEX TERMS

Primary Classification:
C. Computer Systems Organization
C.2 COMPUTER-COMMUNICATION NETWORKS
C.2.1 Network Architecture and Design
Subjects: Wireless communication

General Terms:
Performance

Keywords:
Mobile commerce, infrastructure dependability, location management, mobile applications, satellites,

wireless Internet, wireless LANs, wireless multicast

Peer to Peer - Readers of this Article have also read:

- Efficient and effective placement for very large circuits
  Proceedings of the 1993 IEEE/ACM international conference on Computer-aided design
  Wern-Jieh Sun , Carl Sechen

- The CAVE: audio visual experience automatic virtual environment
  Communications of the ACM 35, 6
  Carolina Cruz-Neira , Daniel J. Sandin , Thomas A. DeFanti , Robert V. Kenyon , John C. Hart

- Clustering and linear placement
  Proceedings of the ninth design automation workshop on Design automation
  Donald M. Schuler , Ernst G. Ulrich

- Editorial pointers
  Communications of the ACM 44, 9
  Diane Crawford

- Resolving semantic heterogeneity in schema integration
  Proceedings of the international conference on Formal Ontology in Information Systems
  Farshad Hakimpour , Andreas Geppert

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2003 ACM, Inc.

PORTAL
THE ACM DIGITAL LIBRARY

> home > about > feedback > login

US Patent & Trademark Office

Try the *new* Portal design
Give us your opinion after using it.

Citation

Mobile Networks and Applications >archive
Volume 8 , Issue 2 (April 2003) >toc

Security in mobile computing environments

A secure infrastructure for service discovery and access in pervasive computing

Authors

Jeffrey Undercoffer Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD

Filip Perich Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD

Andrej Cedilnik Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD

Lalana Kagal Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD

Anupam Joshi Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD

Publisher

ACM Press New York, NY, USA

Pages: 113 - 125 Periodical-Issue-Article
Year of Publication: 2003
ISSN:1383-469X

http://doi.acm.org/10.1145/772052.772054 (Use this link to Bookmark this page)

> full text > abstract > references > index terms > peer to peer

> Discuss > Similar > Review this Article Save to Binder

> BibTex Format

FULL TEXT: Access Rules

pdf 308 KB

ABSTRACT

Security is paramount to the success of pervasive computing environments. The system presented in this

paper provides a communications and security infrastructure that goes far in advancing the goal of anywhere-anytime computing. Our work securely enables clients to access and utilize services in heterogeneous networks. We provide a service registration and discovery mechanism implemented through a hierarchy of service management. The system is built upon a simplified Public Key Infrastructure that provides for authentication, non-repudiation, anti-playback, and access control. Smartcards are used as secure containers for digital certificates. The system is implemented in Java and we use Extensible Markup Language as the sole medium for communications and data exchange. Currently, we are solely dependent on a base set of access rights for our distributed trust model however, we are expanding the model to include the delegation of rights based upon a predefined policy. In our proposed expansion, instead of exclusively relying on predefined access rights, we have developed a flexible representation of trust information, in Prolog, that can model permissions, obligations, entitlements, and prohibitions. In this paper, we present the implementation of our system and describe the modifications to the design that are required to further enhance distributed trust. Our implementation is applicable to any distributed service infrastructure, whether the infrastructure is wired, mobile, or ad hoc.

↑ REFERENCES

Note: OCR errors may be found in this Reference List extracted from the full text article. ACM has opted to expose the complete List rather than only correct and linked references.

1 [1] M. Blaze, J. Feigenbaum and J. Lacy, Decentralized trust management, in: *Proceedings of the 17th IEEE Symposium* (1996).

2 [2] G. Candea and A. Fox, Using dynamic mediation to integrate cots entities in a ubiquitous computing environment, in: *Second International Symposium on Handheld and Ubiquitous Computing 2000* (2000) pp. 248-254.

3 [3] M. Esler, J. Hightower, T. Anderson and G. Borriello, Next century challenges: Data-centric networking for invisible computing, in: *Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom-99)*, August 15-20 (ACM Press, New York, 1999) pp. 256-262.

4 [4] I. Goldberg, S.D. Gribble, D. Wagner and E.A. Brewer, The Ninja jukebox, in: *Proceedings of the 2nd USENIX Symposium on Internet Technologies and Systems (USITS-99)*, Berkeley, CA, USENIX Association (October 11-14, 1999) pp. 37-46.

5 [5] S.D. Gribble et al., The Ninja architecture for robust Internet-scale systems and services, Computer Networks 35(4) (March 2001) 473-497.

6 [6] R. Housley, W. Ford, W. Polk and D. Solo, RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile (Janaury 1999).

7 [7] IETF, Simple public key infrastructure (spki) charter, http://www.ietf.org/html.charters/spkicharter.html

8 [8] L. Kagal, T. Finin and Y. Peng, A framework for distributed trust management, in: *Proceedings of IJCAI-01 Workshop on Autonomy, Delegation and Control* (2001).

9 [9] L. Kagal, V. Korolev, S. Avancha, A. Joshi, T. Finin and Y. Yesha, Highly adaptable infrastructure for service discovery and management in ubiquitous computing, Technical report, TR CS-01-06, Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County,

Baltimore, MD (2001).

10 [10] L. Kagal, V. Korolev, H. Chen, A. Joshi and T. Finin, Project Centaurus: A framework for indoor services mobile services, in: *Proceedings of International Workshop on Smart Appliances and Wearable Computing IWSAWC, in the 21st International Conference on Distributed Computing Systems (ICDCS-21), 2001*, Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD (April 2001).

11 [11] E.C. Lupu, D.A. Marriott, M.S. Sloman and N. Yialelis, A policy based role framework for access control (1995).

12 [12] E. Lupu and M. Sloman, A policy based role object model (1997).

13 [13] Orange and Unisys build the house that listens.

14 [14] R.L. Rivest and B. Lampson, SDSI - A simple distributed security infrastructure, presented at CRYPTO'96 Rumpsession (1996).

15 [15] RSA Laboratories, PKCS 11-cryptographic token interface standard (January 1994).

16 [16] P.R. Zimmermann, *The Official PGP User's Guide* (MIT Press, Cambridge, MA, 1995)

INDEX TERMS

Primary Classification:

C. Computer Systems Organization
- **C.2** COMPUTER-COMMUNICATION NETWORKS
  - **C.2.0** General
    - **Subjects:** Security and protection (e.g., firewalls)

Additional Classification:

C. Computer Systems Organization
- **C.2** COMPUTER-COMMUNICATION NETWORKS
  - **C.2.1** Network Architecture and Design
    - **Subjects:** Wireless communication
  - **C.2.4** Distributed Systems
    - **Subjects:** Distributed applications
- **C.3** SPECIAL-PURPOSE AND APPLICATION-BASED SYSTEMS
  - **Subjects:** Smartcards

I. Computing Methodologies
- **I.7** DOCUMENT AND TEXT PROCESSING
  - **I.7.2** Document Preparation
    - **Subjects:** Markup languages

General Terms:
Design, Languages, Management, Security

Keywords:
distributed services, extensible markup language, pervasive computing, security, smartcards

↑ Peer to Peer - Readers of this Article have also read:

- Data structures for quadtree approximation and compression
  Communications of the ACM 28, 9
  Hanan Samet
- The state of the art in automating usability evaluation of user interfaces
  ACM Computing Surveys (CSUR) 33, 4
- A lifecycle process for the effective reuse of commercial off-the-shelf (COTS) software
  Proceedings of the 1999 symposium on Software reusability
  Christine L. Braun
- Using adapters to reduce interaction complexity in reusable component-based software development
  Proceedings of the 1999 symposium on Software reusability
  David Rine , Nader Nada , Khaled Jaber
- A catalog of techniques for resolving packaging mismatch
  Proceedings of the 1999 symposium on Software reusability
  Robert DeLine

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2003 ACM, Inc.

PORTAL
THE ACM DIGITAL LIBRARY

> home > about > feedback > login

US Patent & Trademark Office

Try the new Portal design
Give us your opinion after using it.

Citation

Wireless Networks >archive
Volume 8 , Issue 2/3 March-May 2002 >toc
Selected Papers from Mobicom'99

An architecture for secure wide-area service discovery

Authors
Todd D. Hodes University of California, Berkeley
Steven E. Czerwinski University of California, Berkeley
Ben Y. Zhao University of California, Berkeley
Anthony D. Joseph University of California, Berkeley
Randy H. Katz University of California, Berkeley

Publisher
Kluwer Academic Publishers Hingham, MA, USA

Pages: 213 - 230 Periodical-Issue-Article
Year of Publication: 2002
ISSN:1022-0038

doi 10.1023/A:1013772027164

> full text > abstract > references > index terms > peer to peer

> Discuss > Similar > Review this Article Save to Binder

> BibTex Format

↑ FULL TEXT: Access Rules

pdf 366 KB

↑ ABSTRACT

The widespread deployment of inexpensive communications technology, computational resources in the networking infrastructure, and network-enabled end devices poses an interesting problem for end users: how to locate a particular network service or device out of hundreds of thousands of accessible services and devices. This paper presents the architecture and implementation of a secure wide-area Service Discovery Service (SDS). Service providers use the SDS to advertise descriptions of available or already running services, while clients use the SDS to compose complex queries for locating these services.

Service descriptions and queries use the eXtensible Markup Language (XML) to encode such factors as cost, performance, location, and device- or service-specific capabilities. The SDS provides a fault-tolerant, incrementally scalable service for locating services in the wide-area. Security is a core component of the SDS: communications are both encrypted and authenticated where necessary, and the system uses a hybrid access control list and capability system to control access to service information. Wide-area query routing is also a core component of the SDS: all information in the system is potentially reachable by all clients.

REFERENCES

Note: OCR errors may be found in this Reference List extracted from the full text article. ACM has opted to expose the complete List rather than only correct and linked references.

1 Elan Amir , Steven McCanne , Randy Katz, An active service framework and its application to real-time multimedia transcoding, Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication, p.178-189, August 31-September 04, 1998, Vancouver, British Columbia, Canada

2 T. Anderson, D. Patterson, D. Culler and the NOW Team, A case for networks of workstations: NOW, IEEE Micro (February 1995).

3 Burton H. Bloom, Space/time trade-offs in hash coding with allowable errors, Communications of the ACM, v.13 n.7, p.422-426, July 1970

4 T. Bray, J. Paoli and C. M. Sperberg-McQueen, eXtensible Markup Language (XML), W3C Recommendation (February 1998) http://www.w3.org/XML

5 Y. Chawathe, S. McCanne and E. Brewer, An architecture for Internet content distribution as an infrastructure service (February 2000) http://www.cs.berkeley.edu/~yatin/papers/

6 Ian Clarke , Oskar Sandberg , Brandon Wiley , Theodore W. Hong, Freenet: a distributed anonymous information storage and retrieval system, International workshop on Designing privacy enhancing technologies: design issues in anonymity and unobservability, p.46-66, January 2001, Berkeley, California, United States

7 Clip 2 Distributed Search Solutions, Bandwidth barriers to Gnutella network scalability, http://dss.clip2.com/dss_barrier.html

8 C. Davis, P. Vixie, T. Goodwin and I. Dickinson, A means for expressing location information in the domain name system, IETF, RFC-1876 (January 1996).

9 S. Deering, Host extensions for IP multicasting, IETF, RFC-1112, SRI International, Menlo Park, CA (August 1989).

10 Stephen Edward Deering, Multicast routing in a datagram internetwork, Stanford University, Stanford, CA, 1992

11 A. Deutsch et al., XML-QL: A query language for XML (August 1998) http://www.w3.org/TR/1998/NOTE-xml-ql-19980819/

12 C. Diot, B. N. Levine, B. Lyles, H. Kassem and D. Balensiefen, Deployment issues for the IP

multicast service and architecture, IEEE Network, Special Issue on Multicasting (January/February 2000).

13 P. Faltstrom, R. Schoultz and C. Weider, How to interact with a WHOIS++ mesh, IETF, RFC-1914 (1995).

14 Li Fan , Pei Cao , Jussara Almeida , Andrei Z. Broder, Summary cache: a scalable wide-area Web cache sharing protocol, Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication, p.254-265, August 31-September 04, 1998, Vancouver, British Columbia, Canada

15 L. Fan, P. Cao, J. Almeida and A. Broder, Summary cache: A scalable wide-area Web cache sharing protocol, Technical report 1361, Computer Sciences Department, University of Wisconsin-Madison (February 1999).

16 S. Fanning, Napster, http://www.napster.com

17 Armando Fox , Steven D. Gribble , Yatin Chawathe , Eric A. Brewer , Paul Gauthier, Cluster-based scalable network services, Proceedings of the sixteenth ACM symposium on Operating systems principles, p.78-91, October 05-08, 1997, Saint Malo, France

18 J. Frankel and T. Pepper, Gnutella, http://gnutella.wego.com

19 Steven D. Gribble , Matt Welsh , Rob von Behren , Eric A. Brewer , David Culler , N. Borisov , S. Czerwinski , R. Gummadi , J. Hill , A. Joseph , R. H. Katz , Z. M. Mao , S. Ross , B. Zhao , Robert C. Holte, The Ninja architecture for robust Internet-scale systems and services373423, Computer Networks: The International Journal of Computer and Telecommunications Networking, v.35 n.4, p.473-497, March 2001

20 E. Guttman and J. Kempf, Automatic discovery of thin servers: SLP, Jini and the SLP-Jini bridge, in: Proceedings of the 25th Annual Conference of the IEEE Industrial Electronics Society (1999) pp. 722-727.

21 E. Guttman, C. Perkins, J. Veizades and M. Day, Service Location Protocol, Version 2, IETF, RFC 2165 (November 1998).

22 M. Handley and V. Jacobson, SDP: Session Description Protocol, IETF, RFC-2327 (1998).

23 Todd D. Hodes , Randy H. Katz, Composable ad hoc location-based services for heterogeneous mobile clients, Wireless Networks, v.5 n.5, p.411-427, Oct. 1999

24 T. Imielinski and S. Goel, DataSpace --- querying and monitoring deeply networked collections in physical space, IEEE Personal Communications Magazine (October 2000).

25 Ravi Jain , Yi-Bing Lin, An auxiliary user location strategy employing forwarding pointers to reduce network impacts of PCS, Wireless Networks, v.1 n.2, p.197-210, 1995

26 David Karger , Eric Lehman , Tom Leighton , Rina Panigrahy , Matthew Levine , Daniel Lewin, Consistent hashing and random trees: distributed caching protocols for relieving hot spots on the World Wide Web, Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, p.654-663, May 04-06, 1997, El Paso, Texas, United States

27 Donald Kossmann , Michael J. Franklin , Gerhard Drasch , Wig Ag, Cache investment: integrating query optimization and distributed data placement, ACM Transactions on Database Systems (TODS), v.25 n.4, p.517-558, Dec. 2000

28 John Kubiatowicz , David Bindel , Yan Chen , Steven Czerwinski , Patrick Eaton , Dennis Geels , Ramakrishna Gummadi , Sean Rhea , Hakim Weatherspoon , Chris Wells , Ben Zhao, OceanStore: an architecture for global-scale persistent storage, Proceedings of the ninth international conference on Architectural support for programming languages and operating systems, p.190-201, November 2000, Cambridge, Massachusetts, United States

29 Brian Neil Levine , Sanjoy Paul , J. J. Garcia-Luna-Aceves, Organizing multicast receivers deterministically by packet-loss correlation, Proceedings of the sixth ACM international conference on Multimedia, p.201-210, September 13-16, 1998, Bristol, United Kingdom

30 M. P. Maher and C. Perkins, Session Announcement Protocol: Version 2, IETF Internet Draft (November 1998) draft-ietf-mmusic-sap-v2-00.txt

31 J. McQuillan, I. Richer and E. Rosen, The new routing algorithm for the ARPANET, IEEE Transactions on Communications 28(5) (May 1980) 711-719.

32 P. Mockapetris , K. J. Dunlap, Development of the domain name system, Symposium proceedings on Communications architectures and protocols, p.123-133, August 16-18, 1988, Stanford, California, United States

33 C. Perkins et al., IP Mobility Support, IETF, RFC 2002 (October 1996).

34 R. Raman, M. Livny and M. Solomon, Matchmaking: Distributed resource management for high throughput computing, in: Proceedings of the Seventh IEEE International Symposium on High Performance Distributed Computing (July 1998).

35 Suchitra Raman , Steven McCanne, A model, analysis, and protocol framework for soft state-based communication, Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication, p.15-25, August 30-September 03, 1999, Cambridge, Massachusetts, United States

36 Sylvia Ratnasamy , Paul Francis , Mark Handley , Richard Karp , Scott Schenker, A scalable content-addressable network, Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications, p.161-172, August 2001, San Diego, California, United States

37 S. Ratnasamy and S. McCanne, Inference of multicast routing trees and bottleneck bandwidths using end-to-end measurements, in: Proceedings of INFOCOM'99 (March 1999).

38 J. Ritter, Why Gnutella can't scale. No, really, http://www.darkridge.com/~jpr5/doc/gnutella.html

39 J. Robie, J. Lapp and D. Schach, XML query language (XQL), in: QL'98 --- The Query Languages Workshop (W3C, December 1998) http://www.w3.org/TandS/QL/QL98/pp/xql.html

40 J. Rosenberg, H. Schulzrinne and B. Suter, Wide area network service location, IETF Draft, Request for Comments (RFC) (December 1997) draft-ietf-svrloc-wasrv-01.txt

41 A. Rousskov and D. Wessels, Cache digests, in: Proceedings of the Third International Web Caching Workshop (June 1998).

42 B. Schneier, Applied Cryptography, 1st ed. (Wiley, 1993).

43 B. Schneier, Description of a new variable-length key, 64-bit block cipher (Blowfish), in: Fast Software Encryption, Cambridge Security Workshop Proceedings (Springer-Verlag, December 1993) pp. 191-204.

44 Michael D. Schroeder , Andrew D. Birrell , Roger M. Needham, Experience with Grapevine: the growth of a distributed system, ACM Transactions on Computer Systems (TOCS), v.2 n.1, p.3-23, February 1984

45 H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson, RTP: A transport protocol for real-time applications, IETF, RFC 1889 (January 1996).

46 S. Seshan, M. Stemm and R. H. Katz, SPAND: Shared passive network performance discovery, in: 1st Usenix Symposium on Internet Technologies and Systems (USITS'97), Monterey, CA (December 1997).

47 Ion Stoica , Robert Morris , David Karger , M. Frans Kaashoek , Hari Balakrishnan, Chord: A scalable peer-to-peer lookup service for internet applications, Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications, p.149-160, August 2001, San Diego, California, United States

48 Sun Microsystems, Jini technology specifications, White paper, http://www.sun.com/jini/specs/

49 M. van Steen, F. Hauck, P. Homburg and A. Tanenbaum, Locating objects in wide-area systems, IEEE Communications Magazine (January 1998) 104-109.

50 Jim Waldo, The Jini architecture for network-centric computing, Communications of the ACM, v.42 n.7, p.76-82, July 1999

51 M. Weiser, The computer for the 21st century, Scientific American 265(3) (September 1991) 94-104.

52 M. Welsh, Ninja RMI, http://www.cs.berkeley.edu/~mdw/proj/ninja/ninjarmi.html

53 D. Wessels and K. Claffy, ICP and the squid Web cache, IEEE Journal on Selected Areas in Communications 16(3) (April 1998) 345-357.

54 L. Wood, V. Apparao et al., Document Object Model Level 1 specification, W3C DOM working group (October 1998) http://www.w3c.org/DOM/

55 B. Zhao, XSet, http://www.cs.berkeley.edu/~ravenben/xset/

56 B. Y. Zhao, J. D. Kubiatowicz and A. D. Joseph, Tapestry: An infrastructure for fault-tolerant wide-area location and routing, Technical report UCB/CSD-01-1141, University of California at Berkeley, Computer Science Division (April 2001).

↑ INDEX TERMS

Primary Classification:
C. Computer Systems Organization
↳ C.2 COMPUTER-COMMUNICATION NETWORKS
↳ C.2.5 Local and Wide-Area Networks

Additional Classification:
C. Computer Systems Organization
↳ C.2 COMPUTER-COMMUNICATION NETWORKS
↳ C.2.1 Network Architecture and Design
↳ **Subjects:** Wireless communication
↳ C.2.2 Network Protocols

General Terms:
Algorithms, Performance, Security

Keywords:
location services, name lookup, network protocols, service discovery

↑ Peer to Peer - Readers of this Article have also read:

- Data structures for quadtree approximation and compression
  Communications of the ACM 28, 9
  Hanan Samet
- The state of the art in automating usability evaluation of user interfaces
  ACM Computing Surveys (CSUR) 33, 4
- A lifecycle process for the effective reuse of commercial off-the-shelf (COTS) software
  Proceedings of the 1999 symposium on Software reusability
  Christine L. Braun
- Using adapters to reduce interaction complexity in reusable component-based software development
  Proceedings of the 1999 symposium on Software reusability
  David Rine , Nader Nada , Khaled Jaber
- A catalog of techniques for resolving packaging mismatch
  Proceedings of the 1999 symposium on Software reusability
  Robert DeLine

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2003 ACM, Inc.

L Number	Hits	Search Text	DB	Time stamp
1	2	(("5764770") or ("5499294")).PN.	USPAT	2004/04/06 09:43
2	339	348/207.99.ccls.	USPAT	2004/04/06 08:55
3	458	380/200.ccls. or 380/258.ccls. or 380/54.ccls. or 380/46.ccls	USPAT	2004/04/06 08:56
4	933	713/176.ccls. or 713/161.ccls. or 713/168.ccls.	USPAT	2004/04/06 08:57
5	2133	713/176.ccls. or 713/161.ccls. or 713/168.ccls. or 713/200.ccls.	USPAT	2004/04/06 08:57
6	664	382/312.ccls. or 382/276.ccls.	USPAT	2004/04/06 08:59
7	585	382/313.ccls. or 382/276.ccls.	USPAT	2004/04/06 08:59
8	879	(382/312.ccls. or 382/276.ccls.) or (382/313.ccls. or 382/276.ccls.)	USPAT	2004/04/06 08:59
9	3694	((382/312.ccls. or 382/276.ccls.) or (382/313.ccls. or 382/276.ccls.)) or (713/176.ccls. or 713/161.ccls. or 713/168.ccls. or 713/200.ccls.) or (380/200.ccls. or 380/258.ccls. or 380/54.ccls. or 380/46.ccls) or 348/207.99.ccls.	USPAT	2004/04/06 09:00
10	1	("6269446").PN.	USPAT	2004/04/06 09:31
11	42737	tight$4 near3 (coupl$4 or attach$5 or connect$4)	USPAT	2004/04/06 09:47
12	113621	sensor and memor$4	USPAT	2004/04/06 09:46
13	1044	(tight$4 near3 (coupl$4 or attach$5 or connect$4)) and (sensor and memor$4)	USPAT	2004/04/06 09:44
14	1707	(authenticat$4 or digital adj2 signature) and (sensor and memor$4)	USPAT	2004/04/06 09:47
15	22	((tight$4 near3 (coupl$4 or attach$5 or connect$4)) and (sensor and memor$4)) and ((authenticat$4 or digital adj2 signature) and (sensor and memor$4))	USPAT	2004/04/06 09:45
16	160881	sensor and memor$4	USPAT; EPO; JPO; DERWENT	2004/04/06 09:45
17	160881	sensor and memor$4	USPAT; EPO; JPO; DERWENT	2004/04/06 09:46
18	41500	authenticat$4 or digital adj2 signature	USPAT; EPO; JPO; DERWENT	2004/04/06 09:47
19	1868	(sensor and memor$4) and (authenticat$4 or digital adj2 signature)	USPAT; EPO; JPO; DERWENT	2004/04/06 09:47
20	61481	tight$4 near3 (coupl$4 or attach$5 or connect$4)	USPAT; EPO; JPO; DERWENT	2004/04/06 09:48
21	22	((sensor and memor$4) and (authenticat$4 or digital adj2 signature)) and (tight$4 near3 (coupl$4 or attach$5 or connect$4))	USPAT; EPO; JPO; DERWENT	2004/04/06 09:48
22	19	(((382/312.ccls. or 382/276.ccls.) or (382/313.ccls. or 382/276.ccls.)) or (713/176.ccls. or 713/161.ccls. or 713/168.ccls. or 713/200.ccls.) or (380/200.ccls. or 380/258.ccls. or 380/54.ccls. or 380/46.ccls) or 348/207.99.ccls.) and (tight$4 near3 (coupl$4 or attach$5 or connect$4))	USPAT; EPO; JPO; DERWENT	2004/04/06 09:48

```
### Status: Path 1 of [Dialog Information Services via Modem]

### Status: Initializing TCP/IP using (UseTelnetProto 1 ServiceID dialog.com)
Trying 31060000009999...Open

DIALOG INFORMATION SERVICES
PLEASE LOGON:
 ******** HHHHHHHH SSSSSSSS?
### Status: Signing onto Dialog
 ********
ENTER PASSWORD:
 ******** HHHHHHHH SSSSSSSS? ********
Welcome to DIALOG
### Status: Connected


Dialog level 04.02.00D

Last logoff:  24mar04 11:16:38
Logon file405 06apr04 08:55:40
           *** ANNOUNCEMENT ***
                  ***
--File 654 - US published applications from March 15, 2001 to the
present are now online.  Please see HELP NEWS 654 for details.

                  ***
--File 581 - The 2003 annual reload of Population Demographics is
complete. Please see Help News581 for details.

                  ***
--File 990 - NewsRoom now contains February 2003 to current records.
File 992 - NewsRoom 2003 archive has been newly created and contains
records from January 2003. The oldest months's records roll out of
File 990 and into File 992 on the first weekend of each month.
To search all 2003 records BEGIN 990, 992, or B NEWS2003, a new
OneSearch category.
                  ***
--Connect Time joins DialUnits as pricing options on Dialog.
See HELP CONNECT for information.
                  ***
                  ***
--SourceOne patents are now delivered to your email inbox
as PDF replacing TIFF delivery. See HELP SOURCE1 for more
information.
                  ***
--Important news for public and academic
libraries.  See HELP LIBRARY for more information.
                  ***
--Important Notice to Freelance Authors--
See HELP FREELANCE for more information
                  ***
NEW FILES RELEASED
***AeroBase (File 104)
***DIOGENES: Adverse Drug Events Database (File 181)
***World News Connection (File 985)
***Dialog NewsRoom - 2003 Archive (File 992)
***TRADEMARKSCAN-Czech Republic (File 680)
***TRADEMARKSCAN-Hungary (File 681)
***TRADEMARKSCAN-Poland  (File 682)
                  ***
UPDATING RESUMED
                  ***
RELOADED
***Medline (Files 154-155)
***Population Demographics -(File 581)
***CLAIMS Citation (Files 220-222)
```

```
REMOVED
                    ***

      >>> Enter BEGIN HOMEBASE for Dialog Announcements <<<
      >>>    of new databases, price changes, etc.       <<<
                    ****
*
*
* ALL NEW CURRENT YEAR RANGES HAVE BEEN * * *
* * * INSTALLED   * * *
SYSTEM:HOME
Cost is in DialUnits
Menu System II: D2 version 1.7.9 term=ASCII
                      *** DIALOG HOMEBASE(SM) Main Menu ***

 Information:
  1.  Announcements (new files, reloads, etc.)
  2.  Database, Rates, & Command Descriptions
  3.  Help in Choosing Databases for Your Topic
  4.  Customer Services (telephone assistance, training, seminars, etc.)
  5.  Product Descriptions

 Connections:
  6.  DIALOG(R) Document Delivery
  7.  Data Star(R)

    (c) 2003 Dialog, a Thomson business.       All rights reserved.

      /H = Help            /L = Logoff           /NOMENU = Command Mode


Enter an option number to view information or to connect to an online
 service.  Enter a BEGIN command plus a file number to search a database
(e.g., B1 for ERIC).
?b 2,6,8,34,434,35,62,77,266,275,621,636,647,674,278,9,696

>>>          77 does not exist
>>>         278 does not exist
>>>2 of the specified files are not available
       06apr04 08:56:42 User264815 Session D50.1
            $0.00    0.157 DialUnits FileHomeBase
     $0.00  Estimated cost FileHomeBase
     $0.50  TELNET
     $0.50  Estimated cost this search
     $0.50  Estimated total session cost   0.157 DialUnits


SYSTEM:OS  - DIALOG OneSearch
  File   2:INSPEC  1969-2004/Mar W4
         (c) 2004 Institution of Electrical Engineers
*File   2: Alert feature enhanced for multiple files, duplicates
removal, customized scheduling. See HELP ALERT.
  File   6:NTIS  1964-2004/Apr W1
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
  File   8:Ei Compendex(R)  1970-2004/Mar W4
         (c) 2004 Elsevier Eng.  Info. Inc.
  File  34:SciSearch(R) Cited Ref Sci  1990-2004/Mar W4
         (c) 2004 Inst for Sci Info
  File 434:SciSearch(R) Cited Ref Sci  1974-1989/Dec
         (c) 1998 Inst for Sci Info
  File  35:Dissertation Abs Online  1861-2004/Mar
         (c) 2004 ProQuest Info&Learning
  File  62:SPIN(R)  1975-2004/Feb W3
         (c) 2004 American Institute of Physics
  File 266:FEDRIP  2004/Feb
         Comp & dist by NTIS, Intl Copyright All Rights Res
```

```
  File 275:Gale Group Computer DB(TM)  1983-2004/Apr 06
         (c) 2004 The Gale Group
  File 621:Gale Group New Prod.Annou.(R)  1985-2004/Apr 06
         (c) 2004 The Gale Group
  File 636:Gale Group Newsletter DB(TM)  1987-2004/Apr 06
         (c) 2004 The Gale Group
  File 647:CMP  Computer Fulltext  1988-2004/Mar W4
         (c) 2004 CMP Media, LLC
  File 674:Computer News Fulltext  1989-2004/Apr W1
         (c) 2004 IDG Communications
  File   9:Business & Industry(R)  Jul/1994-2004/Apr 02
         (c) 2004  The Gale Group
  File 696:DIALOG Telecom. Newsletters  1995-2004/Apr 05
         (c) 2004 The Dialog Corp.

      Set  Items  Description
      ---  -----  -----------
?s camera? or image (3n) device
          274815  CAMERA?
         1062779  IMAGE
         1200365  DEVICE
            5084  IMAGE(3N)DEVICE
      S1  278438  CAMERA? OR IMAGE (3N) DEVICE
?s tight? (3n) coupl?
          359209  TIGHT?
         1516955  COUPL?
      S2   12630  TIGHT? (3N) COUPL?
?s sensor? (s) s2
          682317  SENSOR?
           12630  S2
      S3     255  SENSOR? (S) S2
?s authenticat? or digital (2n) signature or validat?
           76247  AUTHENTICAT?
         1758945  DIGITAL
          126140  SIGNATURE
           10124  DIGITAL(2N)SIGNATURE
          411342  VALIDAT?
      S4  487830  AUTHENTICAT? OR DIGITAL (2N) SIGNATURE OR VALIDAT?
?s s3 and s4
             255  S3
          487830  S4
      S5      21  S3 AND S4
?s s1 and s4
          278438  S1
          487830  S4
      S6    5333  S1 AND S4
?s s1 and s2
          278438  S1
           12630  S2
      S7     189  S1 AND S2
?s s4 and s2
          487830  S4
           12630  S2
      S8     623  S4 AND S2
?s GPS and s1
           66150  GPS
          278438  S1
      S9    2711  GPS AND S1
?s s9 and s4
            2711  S9
          487830  S4
     S10     153  S9 AND S4
?s s4 and s10
          487830  S4
             153  S10
     S11     153  S4 AND S10
?s s2 (s) s3
```

```
        12630  S2
          255  S3
S12       255  S2 (S) S3
```

L Number	Hits	Search Text	DB	Time stamp
1	637	(compar$4 or verif$4) near4 (digital adj1 signature)	USPAT	2003/08/12 10:41
2	968	(compar$4 or verif$4 or authenticat$4) near4 (digital adj1 signature)	USPAT	2003/08/12 10:41
3	60582	(digital adj1 camera) or (digital adj1 picture) or (digital adj1 image) or (data near2 stream$4)	USPAT	2003/08/12 10:43
4	582001	parameter or GPS or ID or coordinate or compass or ID	USPAT	2003/08/12 10:44
5	208	(parameter or GPS or ID or coordinate or compass or ID) and ((digital adj1 camera) or (digital adj1 picture) or (digital adj1 image) or (data near2 stream$4)) and ((compar$4 or verif$4 or authenticat$4) near4 (digital adj1 signature))	USPAT	2003/08/12 10:51
6	724	(parameter or GPS or ID or coordinate or compass or ID) and ((compar$4 or verif$4 or authenticat$4) near4 (digital adj1 signature))	USPAT	2003/08/12 10:51
7	18	((parameter or GPS or ID or coordinate or compass or ID) and ((compar$4 or verif$4 or authenticat$4) near4 (digital adj1 signature))) and GPS	USPAT	2003/08/12 11:01
8	18	((parameter or GPS or ID or coordinate or compass or ID) and ((compar$4 or verif$4 or authenticat$4) near4 (digital adj1 signature))) and GPS	USPAT; EPO; DERWENT	2003/08/12 11:01

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

7590 04/20/2004

Welsh & Katz
120 south Riverside Plaza
22nd Floor
Chicago, IL 60606

EXAMINER	
SONG, HOSUK	
ART UNIT	PAPER NUMBER
2135	8

DATE MAILED: 04/20/2004

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/626,044	07/27/2000	Jonathan E. Jaffe	6468/78445	9426

TITLE OF INVENTION: INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$665	$0	$665	07/20/2004

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

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE REFLECTS A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE APPLIED IN THIS APPLICATION. THE PTOL-85B (OR AN EQUIVALENT) MUST BE RETURNED WITHIN THIS PERIOD EVEN IF NO FEE IS DUE OR THE APPLICATION WILL BE REGARDED AS ABANDONED.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:
A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status is changed, pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above and notify the United States Patent and Trademark Office of the change in status, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check the box below and enclose the PUBLICATION FEE and 1/2 the ISSUE FEE shown above.

☐ Applicant claims SMALL ENTITY status.
See 37 CFR 1.27.

II. PART B - FEE(S) TRANSMITTAL should be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). Even if the fee(s) have already been paid, Part B - Fee(s) Transmittal should be completed and returned. If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted.

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

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 11/03) Approved for use through 04/30/2004.

ADOBE – Exhibit 1002, page 314
JAFFE-ADOBE000348

Notice of Allowability	Application No.	Applicant(s)	
	09/626,044	JAFFE ET AL.	
	Examiner	Art Unit	
	Hosuk Song	2135	

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

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

1. ☒ This communication is responsive to *amendment filed 3/11/2004*.

2. ☒ The allowed claim(s) is/are *9-14*.

3. ☒ The drawings filed on *7/27/2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____.
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

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

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

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

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

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.
7. ☐ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (703) 746-4000

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 4 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Legibly mark-up with any corrections or use Block 1)

7590 04/20/2004

Welsh & Katz
120 south Riverside Plaza
22nd Floor
Chicago, IL 60606

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

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/626,044	07/27/2000	Jonathan E. Jaffe	6468/78445	9426

TITLE OF INVENTION: INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$665	$0	$665	07/20/2004

EXAMINER	ART UNIT	CLASS-SUBCLASS
SONG, HOSUK	2135	713-176000

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

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

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

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

1 _____
2 _____
3 _____

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the USPTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.

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

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ individual ☐ corporation or other private group entity ☐ government

4a. The following fee(s) are enclosed:

☐ Issue Fee
☐ Publication Fee
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s):

☐ A check in the amount of the fee(s) is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

Director for Patents is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.

(Authorized Signature) (Date)

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMIT THIS FORM WITH FEE(S)

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/626,044	07/27/2000	Jonathan E. Jaffe	6468/78445	9426

7590 04/20/2004

Welsh & Katz
120 south Riverside Plaza
22nd Floor
Chicago, IL 60606

EXAMINER	
SONG, HOSUK	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/20/2004

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

The Patent Term Adjustment to date is 706 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 706 day(s).

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

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

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (703) 305-1383. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (703) 305-8283.

PTOL-85 (Rev. 11/03) Approved for use through 04/30/2004.

ADOBE – Exhibit 1002, page 317
JAFFE-ADOBE000351

OIPE
APR 26 2004
PATENT & TRADEMARK OFFICE

RT B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (703) 746-4000

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 4 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Legibly mark-up with any corrections or use Block 1)

7590 04/20/2004

Welsh & Katz
120 south Riverside Plaza
22nd Floor
Chicago, IL 60606

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

Certificate of Mailing or Transmission

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

Maura Halvey	(Depositor's name)
Maura Halvey	(Signature)
April 26 2004	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/626,044	07/27/2000	Jonathan E. Jaffe	6468/78445	9426

TITLE OF INVENTION: INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$665	$0	$665	07/20/2004

EXAMINER	ART UNIT	CLASS-SUBCLASS
SONG, HOSUK	2135	713-176000

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

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

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

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

1 Welsh & Katz, Ltd.
2
3

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the USPTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.

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

Please check the appropriate assignee category or categories (will not be printed on the patent); ☐ individual ☒ corporation or other private group entity ☐ government

4a. The following fee(s) are enclosed:

☒ Issue Fee
☐ Publication Fee
☒ Advance Order - # of Copies 10

4b. Payment of Fee(s):

☒ A check in the amount of the fee(s) is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number 23-0920 (enclose an extra copy of this form).

Director of Patents is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.

Maura Halvey 26 April 2004
(Authorized Signature) (Date)

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

04/28/2004 HVUONG2 00000033 09626044
01 FC:2501 665.00 OP

04/30/2004 SLUANG2 00000015 230920 09626044
01 FC:8001 30.00 DA

TRANSMIT THIS FORM WITH FEE(S)

ADOBE – Exhibit 1002, page 318
JAFFE-ADOBE000352

TRANSMITTAL OF PAYMENT OF ISSUE FEE (Small Entity) (37 C.F.R. 1.311)	Docket No. 6468/78445

OIPE
APR 26 2004
PATENT & TRADEMARK OFFICE

Applicant(s):
Jonathan E. Jaffe

Serial No.	Filing Date	Examiner	Group Art Unit	Confirmation No.
09/626,044	07/27/2000	Song, Hosuk	2135	9426

Invention: INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES

Mail Stop Issue Fee
TO THE COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Transmitted herewith are the following for the above-identified application.

- ☒ Issue Fee Transmittal Form PTOL-85
- ☒ Utility Fee: $ 665.00 ☐ Design Fee: _____ ☐ Plant Fee: _____
- ☐ Publication Fee: _____
- ☒ A check in the amount of $665.00 is attached.
- ☒ The Director is hereby authorized to charge and credit Deposit Account No. 23-0920 as described below.
  - ☐ Charge the amount of
  - ☒ Credit any overpayment.
  - ☒ Charge any additional fee required.

Jeffrey W. Saunders
Signature

Dated: 26 Apr 2004

I hereby certify that this paper is being deposited with the United States Postal Service as Express Mail in an envelope addressed to: Mail Stop Issue Fee Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this date.
4/26/04 Megan Hall
Date
Express Mail Label No. EV 596734643US

cc:

Certificate of Transmission by Facsimile
This certificate may only be used if paying by deposit account.

I certify that this document and authorization to charge account is being facsimile transmitted to the United States and Trademark Office (Fax) on

Date

Signature

Typed or Printed Name of Person Signing Certificate

Certificate of Mailing by First Class Mail

I certify that this document and fee is being deposited on with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

P355MALL/REV03

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	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
09/626,044	6757828	2135	9200 R |0101 |031 |13

Change of Address/Power of Attorney

The following fields have been set to Customer Number 24628 on

- Correspondence Address
- Power of Attorney

The address of record for Customer Number 24628 is:
WELSH & KATZ, LTD
120 S RIVERSIDE PLAZA
22ND FLOOR
CHICAGO, IL 60606

The Practitioners of record for Customer Number 24628 are:

PTO INSTRUCTIONS:

Please take the following action when the correspondence address has been changed to a customer number:
1) Add 'ADDRESS CHANGE TO CUSTOMER NUMBER' on the next available content line of the File Jacket.
2) Put a line through the old address on the File Jacket and enter the Customer Number as the new address.
3) File this Notice in the File Jacket.

Please take the following action when the correspondence address has NOT been changed:
1) File this Notice in the File Jacket

US006757828B1

(12) **United States Patent**
Jaffe et al.

(10) **Patent No.: US 6,757,828 B1**
(45) **Date of Patent: Jun. 29, 2004**

(54) **INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES**

(76) Inventors: **Jonathan E. Jaffe**, 1003 Bradford Blvd., Gallatin, TN (US) 37066; **Joel D. Goldhar**, 720 Foxdale Ave., Winnetka, IL (US) 60093; **Michael A. Warot**, 532 Florence, Hammond, IN (US) 46324

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 706 days.

(21) Appl. No.: **09/626,044**

(22) Filed: **Jul. 27, 2000**

(51) **Int. Cl.**[7] **H04L 9/00**
(52) **U.S. Cl.** **713/176**; 380/200; 380/258
(58) **Field of Search** 713/176, 168, 713/161, 200; 380/258, 229, 200, 54, 46; 348/207.99; 382/276, 312–313

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,499,294 A * 3/1996 Friedman 713/179
5,504,518 A * 4/1996 Ellis et al. 725/22
5,764,770 A * 6/1998 Schipper et al. 713/176
6,253,337 B1 * 6/2001 Maloney et al. 714/38
6,269,446 B1 * 7/2001 Schumacher et al. 713/176

* cited by examiner

Primary Examiner—Kim Vu
Assistant Examiner—Hosuk Song
(74) *Attorney, Agent, or Firm*—Welsh & Katz, Ltd.

(57) **ABSTRACT**

A method and system of authentication for sensor-recorders and other information capture devices is disclosed. In accordance with aspects of the current invention, a digital sample of the environment is obtained. From this sample and at least one parameter representative of at least one condition under which the sample was generated, a digital signature is created. This signature is stored in memory with the sample to be checked at a later time for authenticity. The file is checked for authenticity by generating a second signature from the file and comparing that signature to the original signature. If the two signatures are identical, the sample is considered authentic and if the two signatures are different, the sample cannot be authenticated.

6 Claims, 21 Drawing Sheets

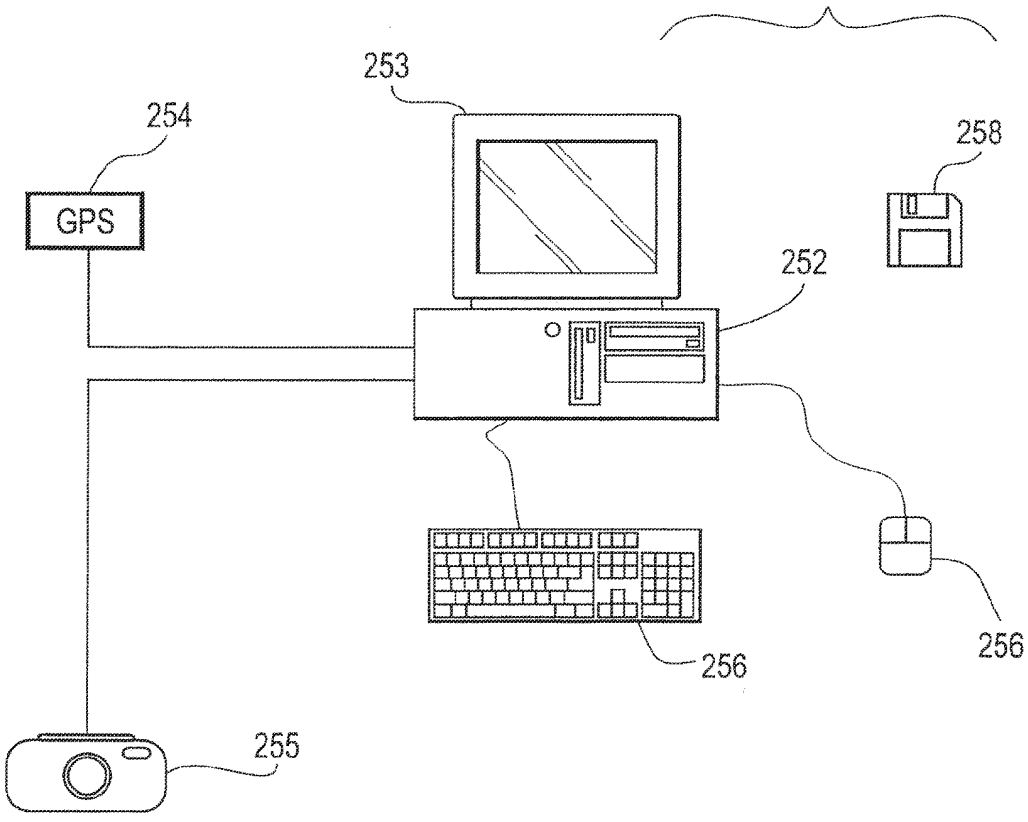


FIG. 1

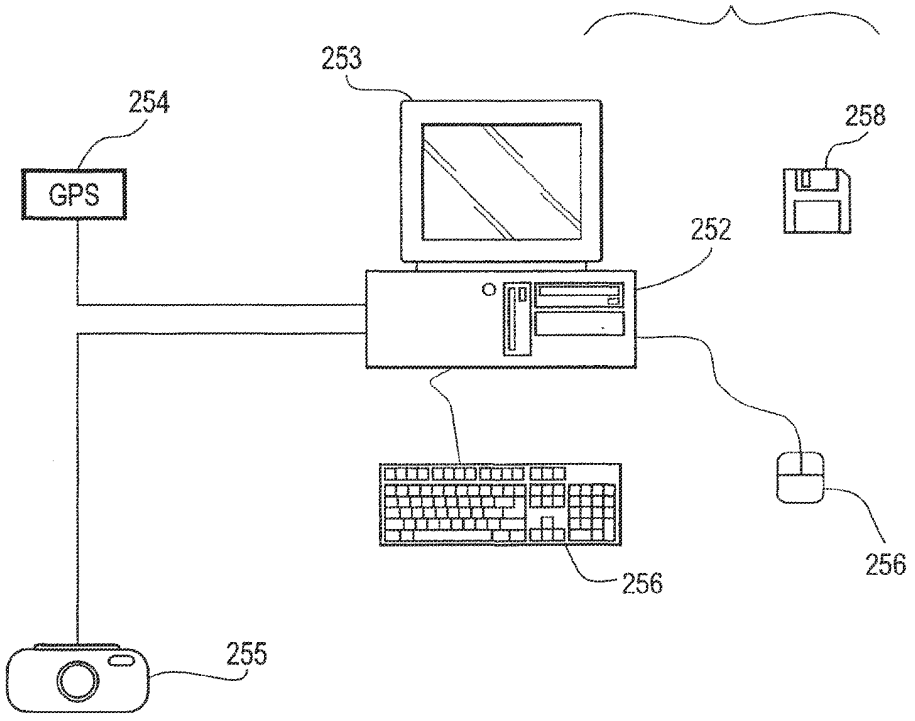


FIG. 2

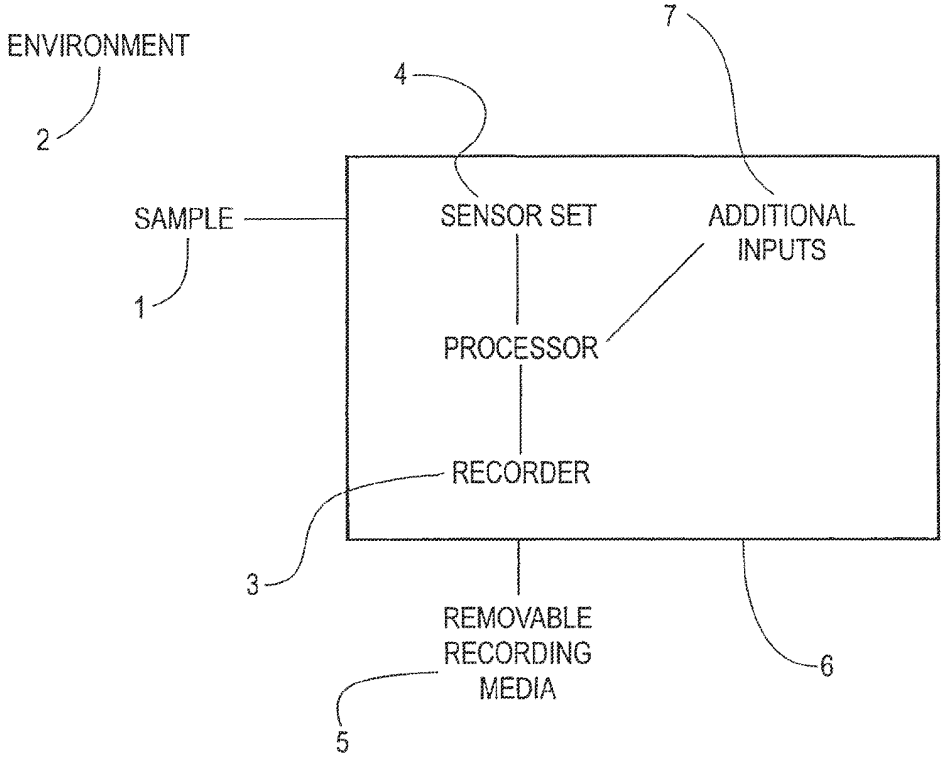
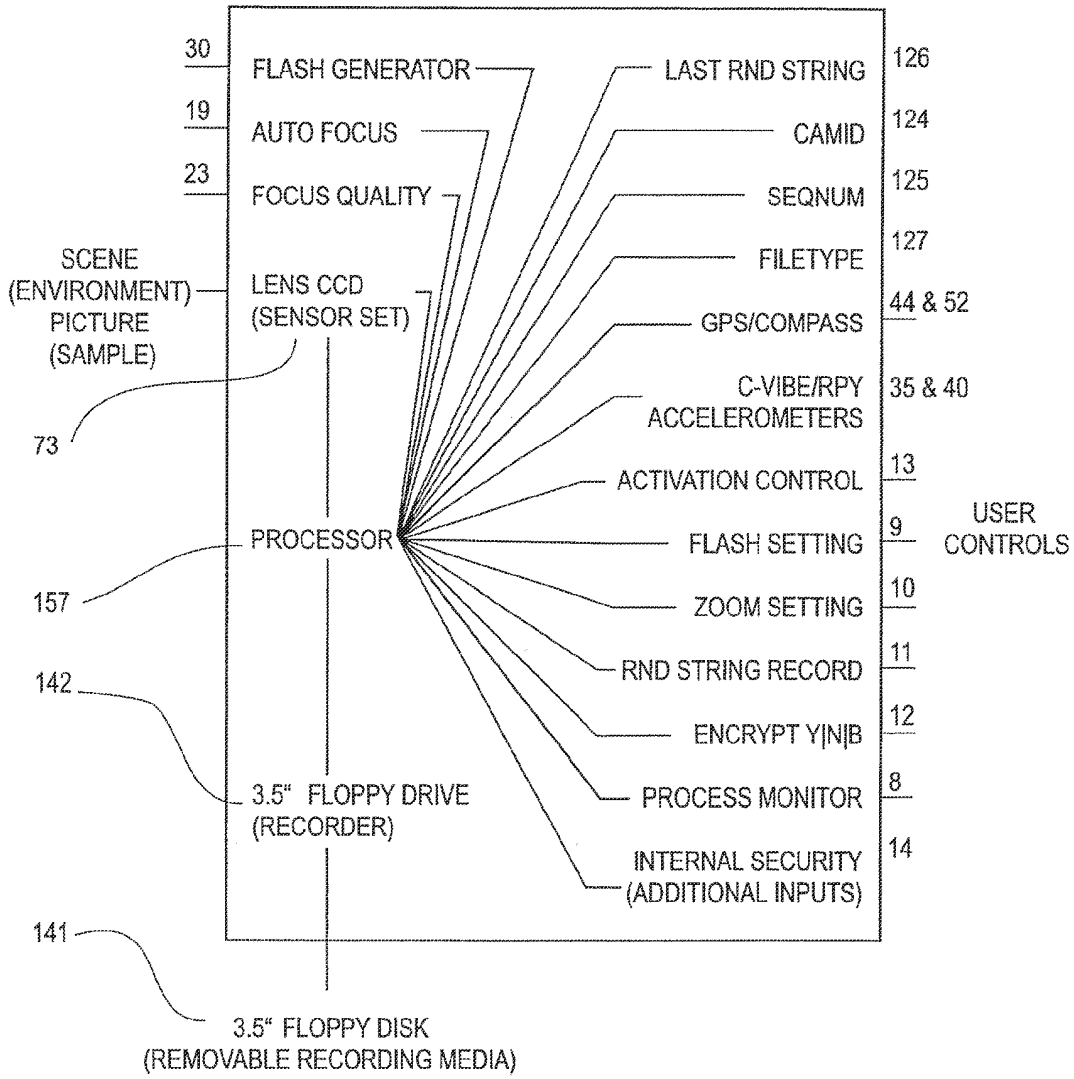

ENVIRONMENT
2
4
7
SAMPLE
1
SENSOR SET
ADDITIONAL INPUTS
PROCESSOR
RECORDER
3
REMOVABLE RECORDING MEDIA
5
6

FIG. 2A



GPS IS GEOPOSITIONING SYSTEM
C-VIBE IS THE COUNTER VIBRATION UNIT
RPY IS ROLL-PITCH YAW DETECTION
CAMID IS CAMERA IDENTIFICATION
SEQNUM IS SEQUENCE NUMBER

FIG. 3

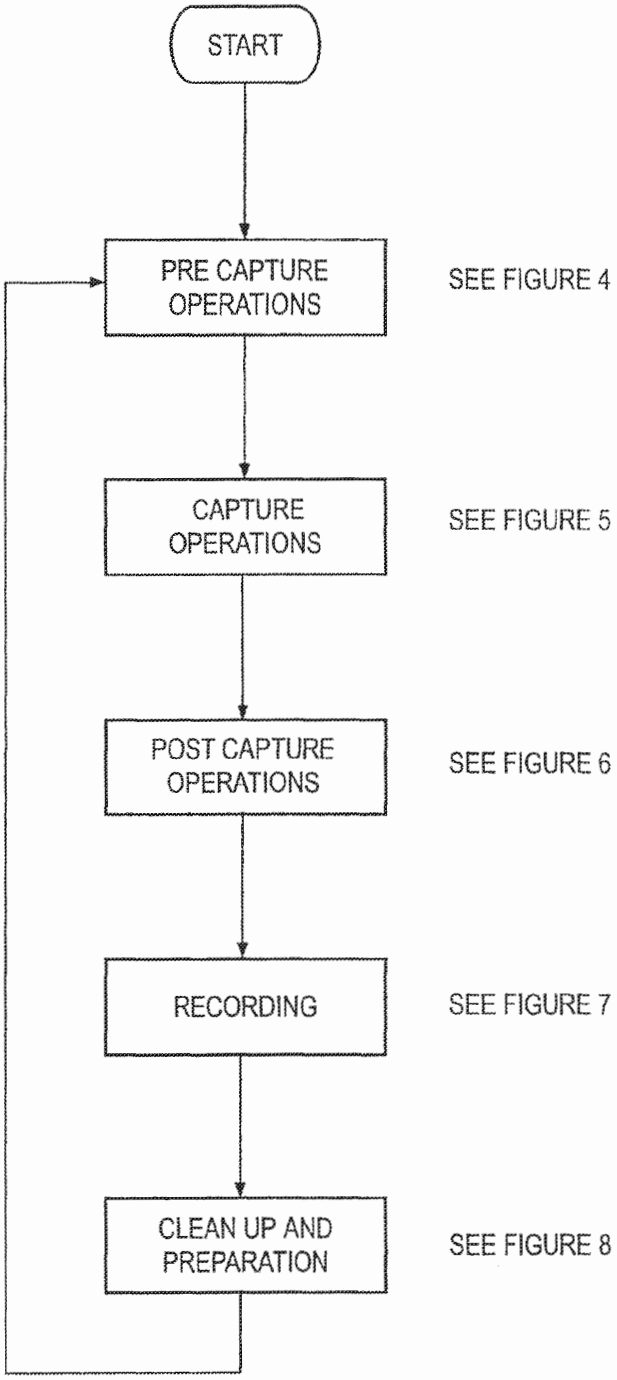
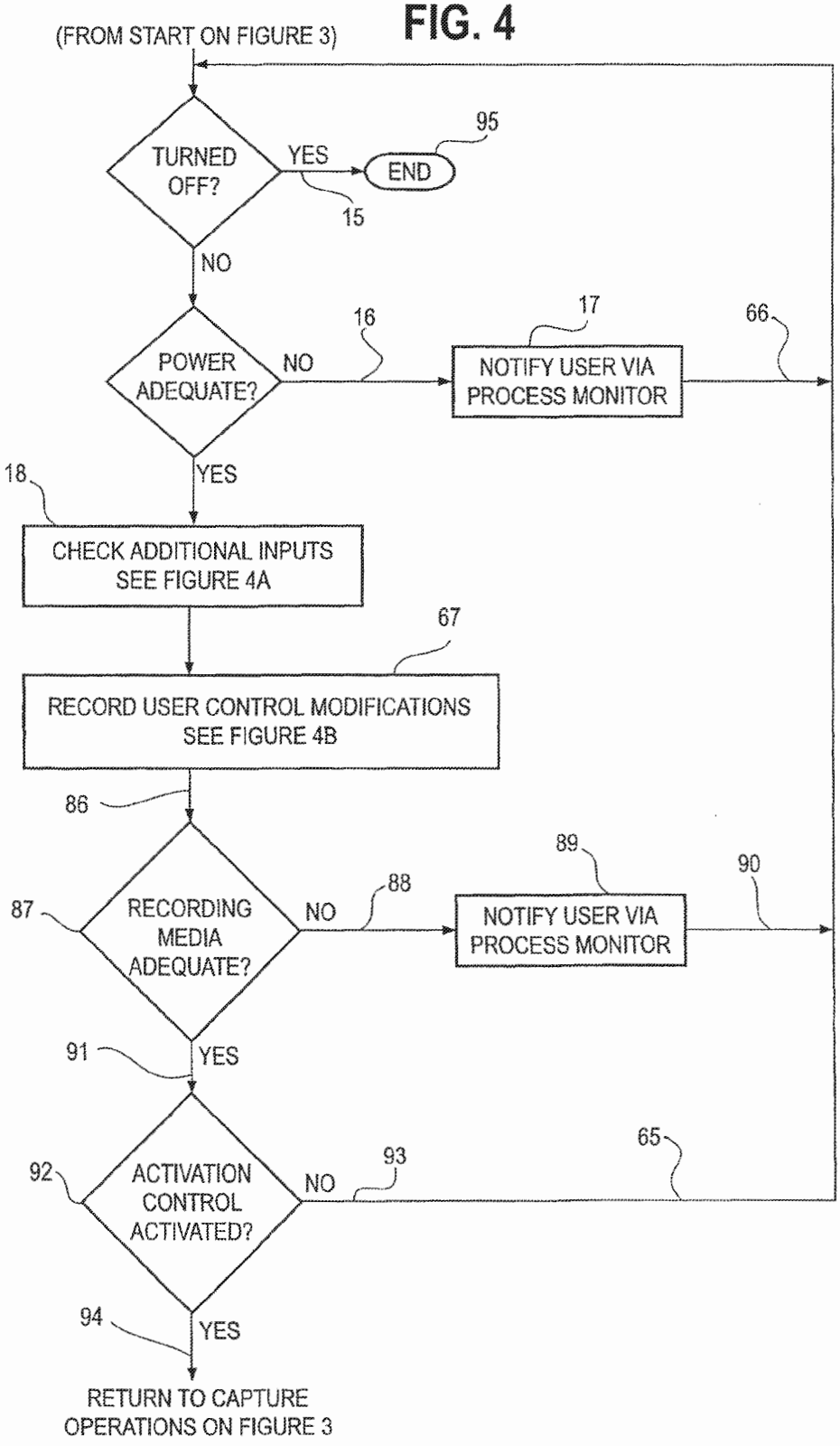

START
PRE CAPTURE OPERATIONS
SEE FIGURE 4
CAPTURE OPERATIONS
SEE FIGURE 5
POST CAPTURE OPERATIONS
SEE FIGURE 6
RECORDING
SEE FIGURE 7
CLEAN UP AND PREPARATION
SEE FIGURE 8

FIG. 4


(FROM START ON FIGURE 3)
TURNED OFF?
YES
END
95
15
NO
POWER ADEQUATE?
NO
16
17
NOTIFY USER VIA PROCESS MONITOR
66
YES
18
CHECK ADDITIONAL INPUTS SEE FIGURE 4A
67
RECORD USER CONTROL MODIFICATIONS SEE FIGURE 4B
86
RECORDING MEDIA ADEQUATE?
87
NO
88
89
NOTIFY USER VIA PROCESS MONITOR
90
91
YES
ACTIVATION CONTROL ACTIVATED?
92
NO
93
65
94
YES
RETURN TO CAPTURE OPERATIONS ON FIGURE 3

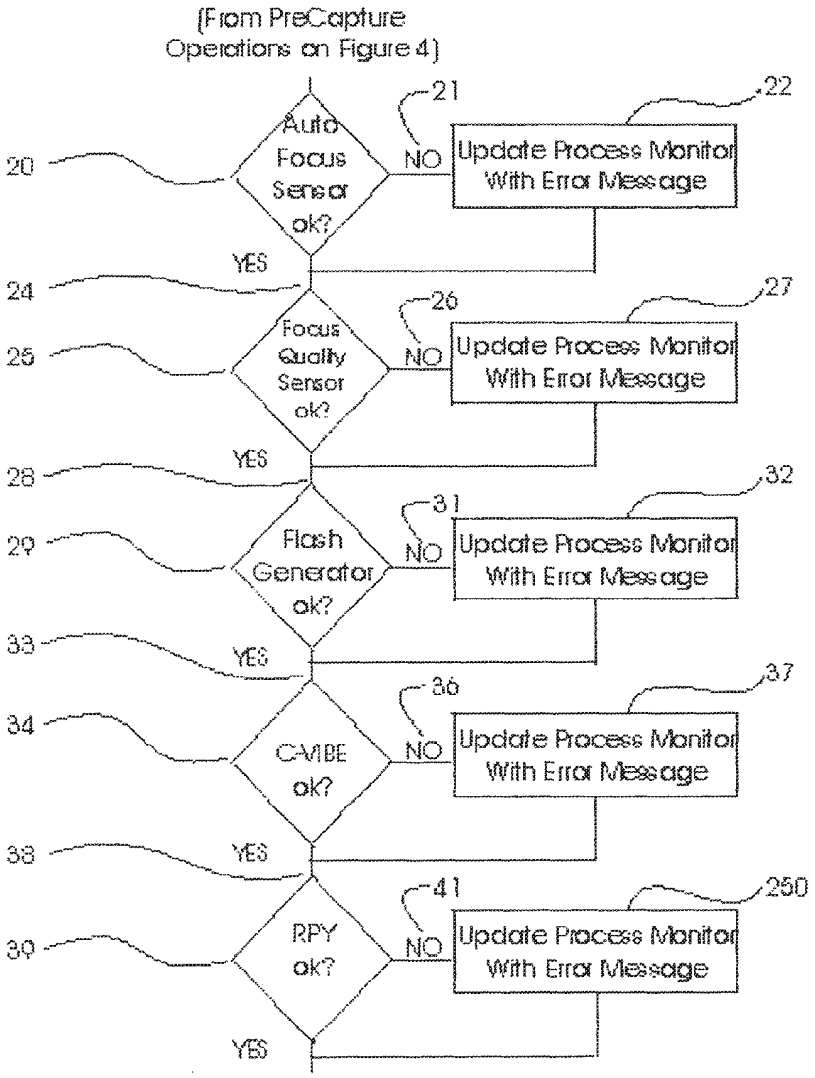

(From PreCapture Operations on Figure 4)
20
Auto Focus Sensor ok?
21
NO
22
Update Process Monitor With Error Message
YES
24
25
Focus Quality Sensor ok?
26
NO
27
Update Process Monitor With Error Message
YES
28
29
Flash Generator ok?
31
NO
32
Update Process Monitor With Error Message
YES
33
34
C-VIBE ok?
36
NO
37
Update Process Monitor With Error Message
YES
38
39
RPY ok?
41
NO
250
Update Process Monitor With Error Message
YES
(Continued on Figure 4A

FIGURE 4A

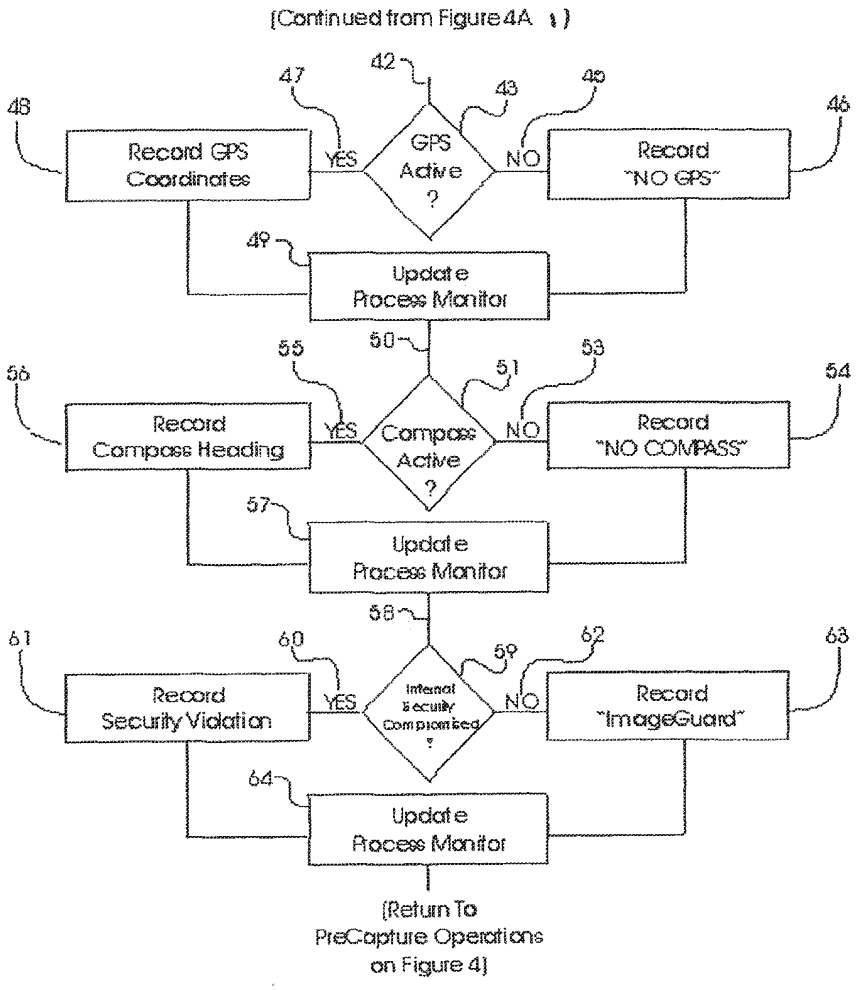

(Continued from Figure 4A 1)
42
47
43
45
48
Record GPS Coordinates
YES
GPS Active ?
NO
Record "NO GPS"
46
49
Update Process Monitor
50
55
51
53
56
Record Compass Heading
YES
Compass Active ?
NO
Record "NO COMPASS"
54
57
Update Process Monitor
58
61
60
59
62
63
Record Security Violation
YES
Internal Security Compromised ?
NO
Record "ImageGuard"
64
Update Process Monitor
(Return To PreCapture Operations on Figure 4)

FIGURE 4A2

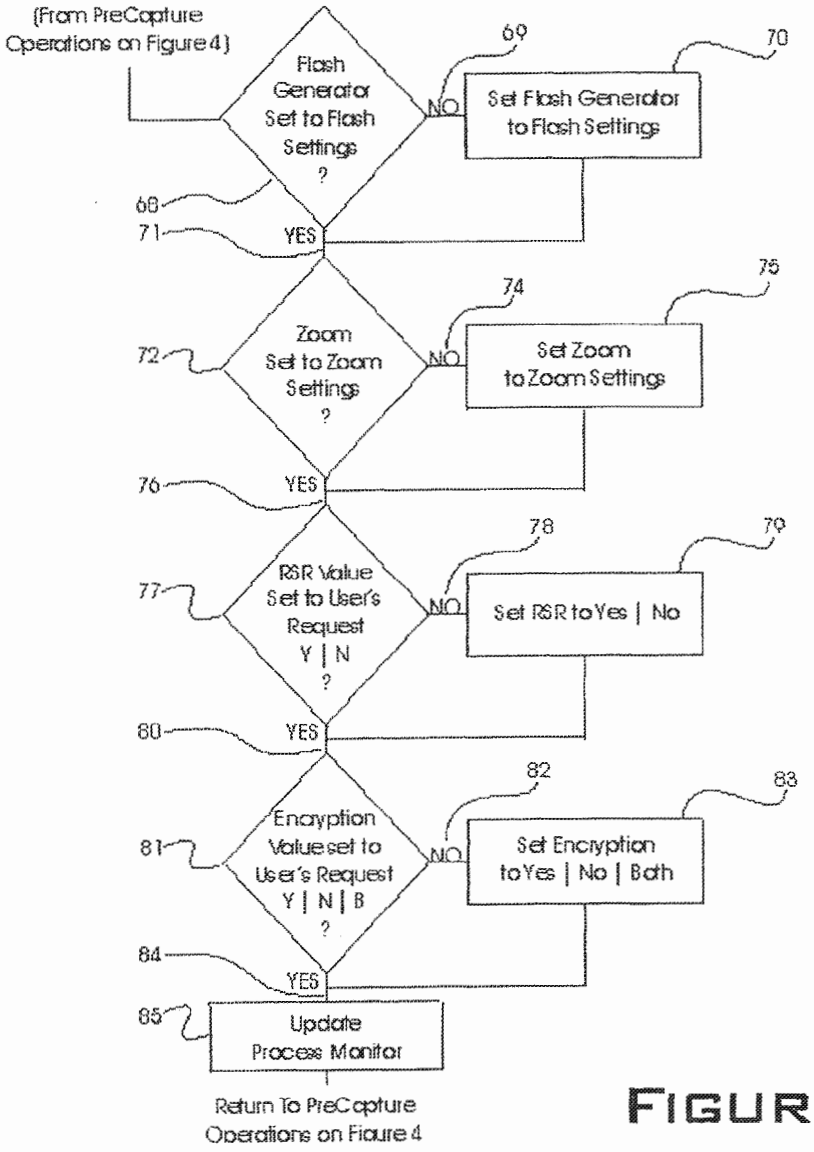

(From PreCapture Operations on Figure 4)
Flash Generator Set to Flash Settings ?
NO
69
Set Flash Generator to Flash Settings
70
68
YES
71
Zoom Set to Zoom Settings ?
72
NO
74
Set Zoom to Zoom Settings
75
YES
76
RSR Value Set to User's Request Y | N ?
77
NO
78
Set RSR to Yes | No
79
YES
80
Encryption Value set to User's Request Y | N | B ?
81
NO
82
Set Encryption to Yes | No | Both
83
YES
84
Update Process Monitor
85
Return To PreCapture Operations on Figure 4

FIGURE 4B

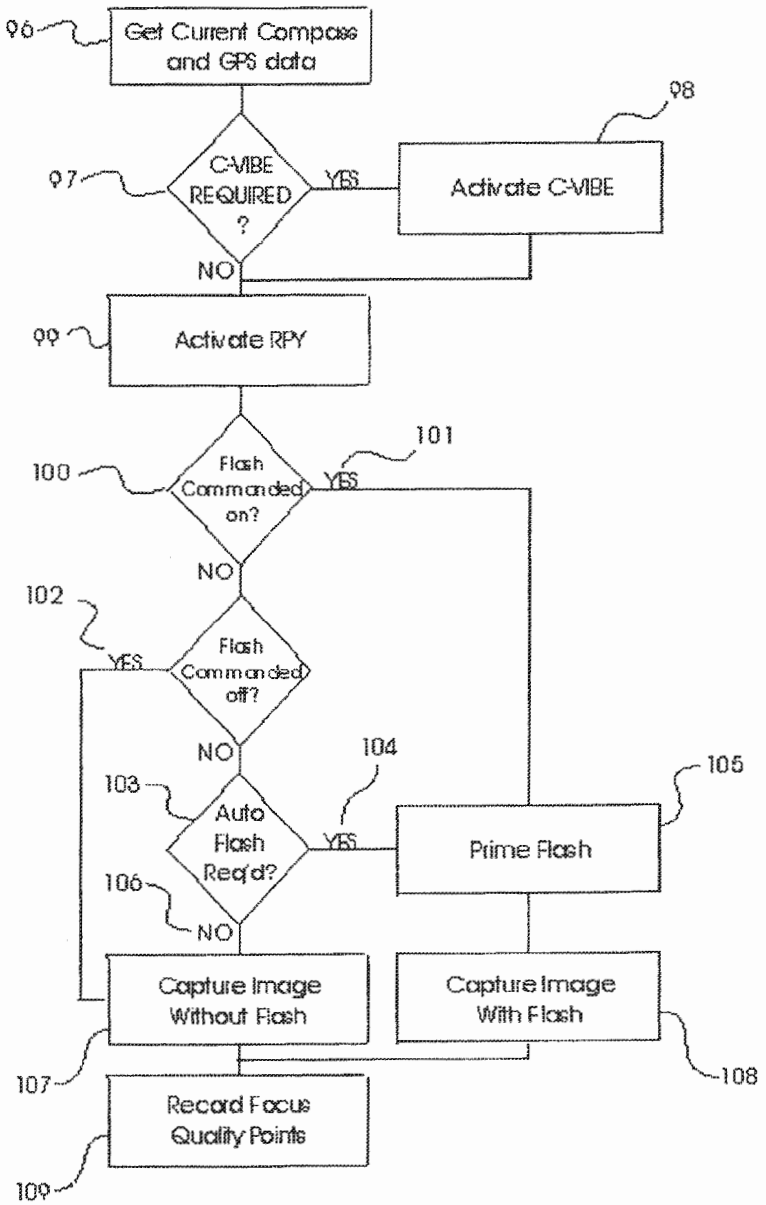
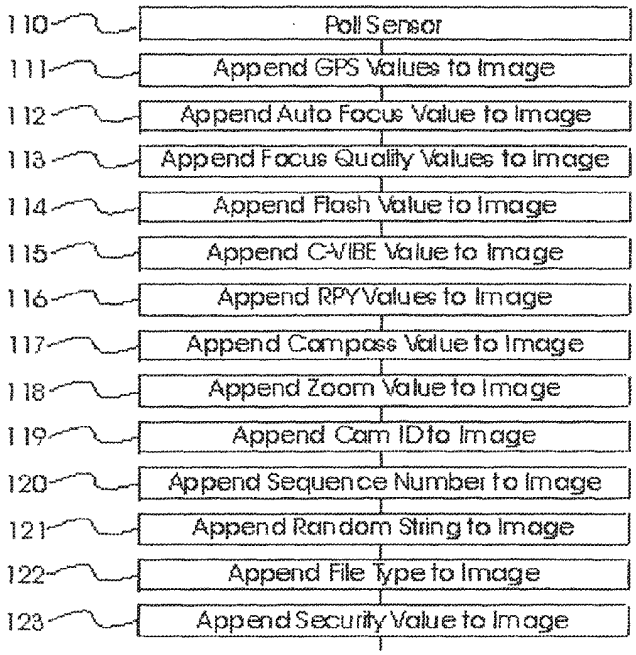

96
Get Current Compass and GPS data
98
97
C-VIBE REQUIRED ?
YES
Activate C-VIBE
NO
99
Activate RPY
101
100
Flash Commanded on?
YES
NO
102
YES
Flash Commanded off?
NO
104
105
103
Auto Flash Req'd?
YES
Prime Flash
106
NO
Capture Image Without Flash
Capture Image With Flash
107
108
Record Focus Quality Points
109

FIGURE 5



(Continued on Figure 6 B)

FIGURE 6

FIG. 6B

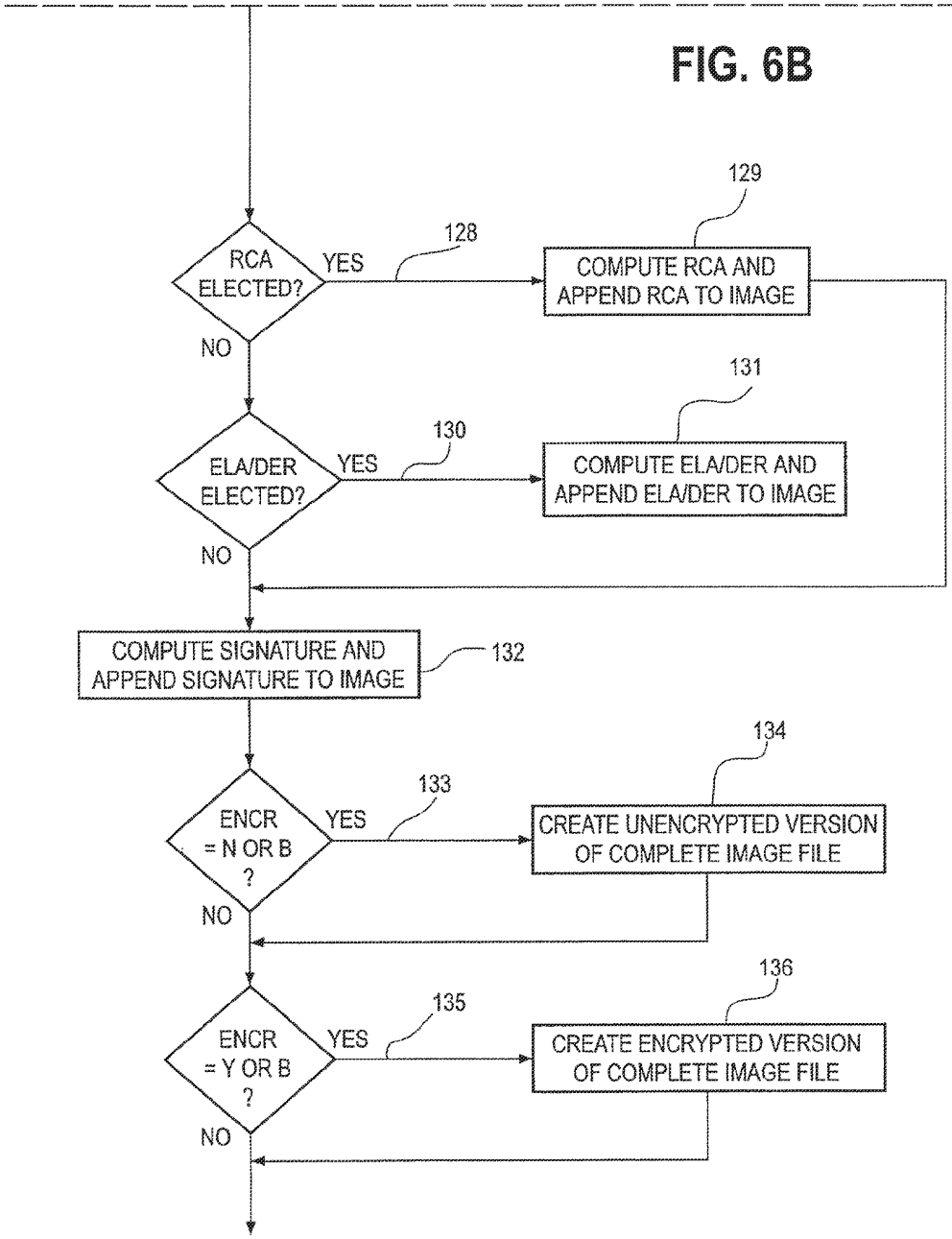

RCA ELECTED?
YES
128
129
COMPUTE RCA AND APPEND RCA TO IMAGE
NO
ELA/DER ELECTED?
YES
130
131
COMPUTE ELA/DER AND APPEND ELA/DER TO IMAGE
NO
COMPUTE SIGNATURE AND APPEND SIGNATURE TO IMAGE
132
ENCR = N OR B ?
YES
133
134
CREATE UNENCRYPTED VERSION OF COMPLETE IMAGE FILE
NO
ENCR = Y OR B ?
YES
135
136
CREATE ENCRYPTED VERSION OF COMPLETE IMAGE FILE
NO
END OF POST CAPTURE OPERATIONS

FIG. 7

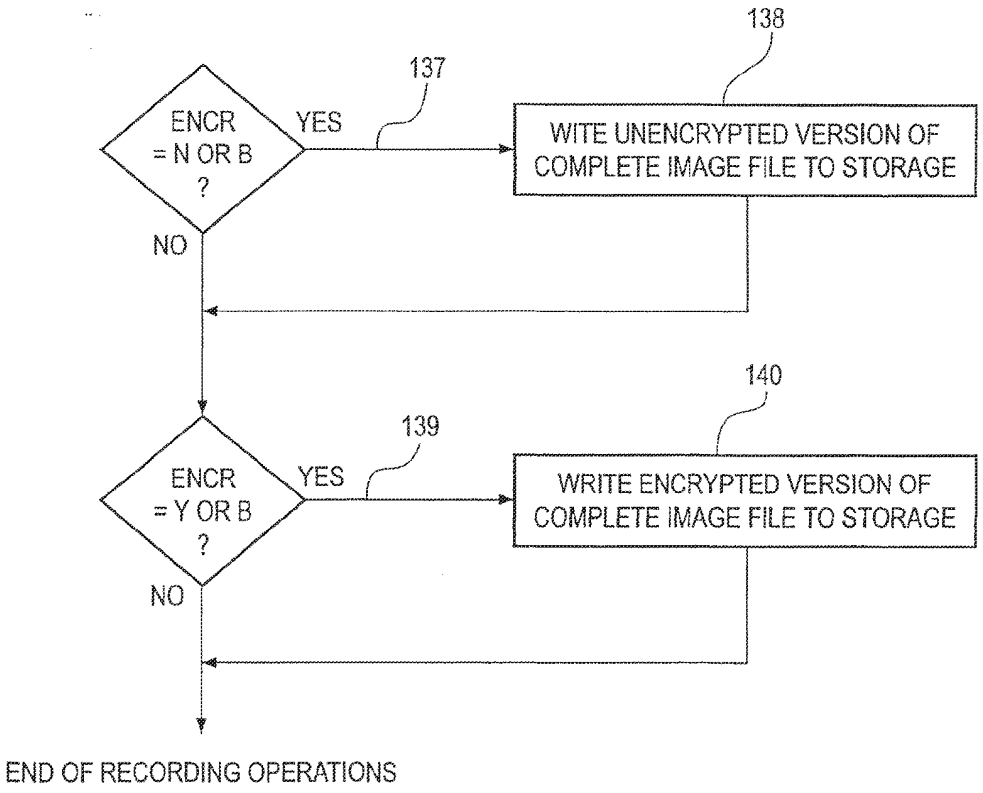

138
137
ENCR
= N OR B
?
YES
WITE UNENCRYPTED VERSION OF
COMPLETE IMAGE FILE TO STORAGE
NO
140
139
ENCR
= Y OR B
?
YES
WRITE ENCRYPTED VERSION OF
COMPLETE IMAGE FILE TO STORAGE
NO
END OF RECORDING OPERATIONS

FIG. 7A

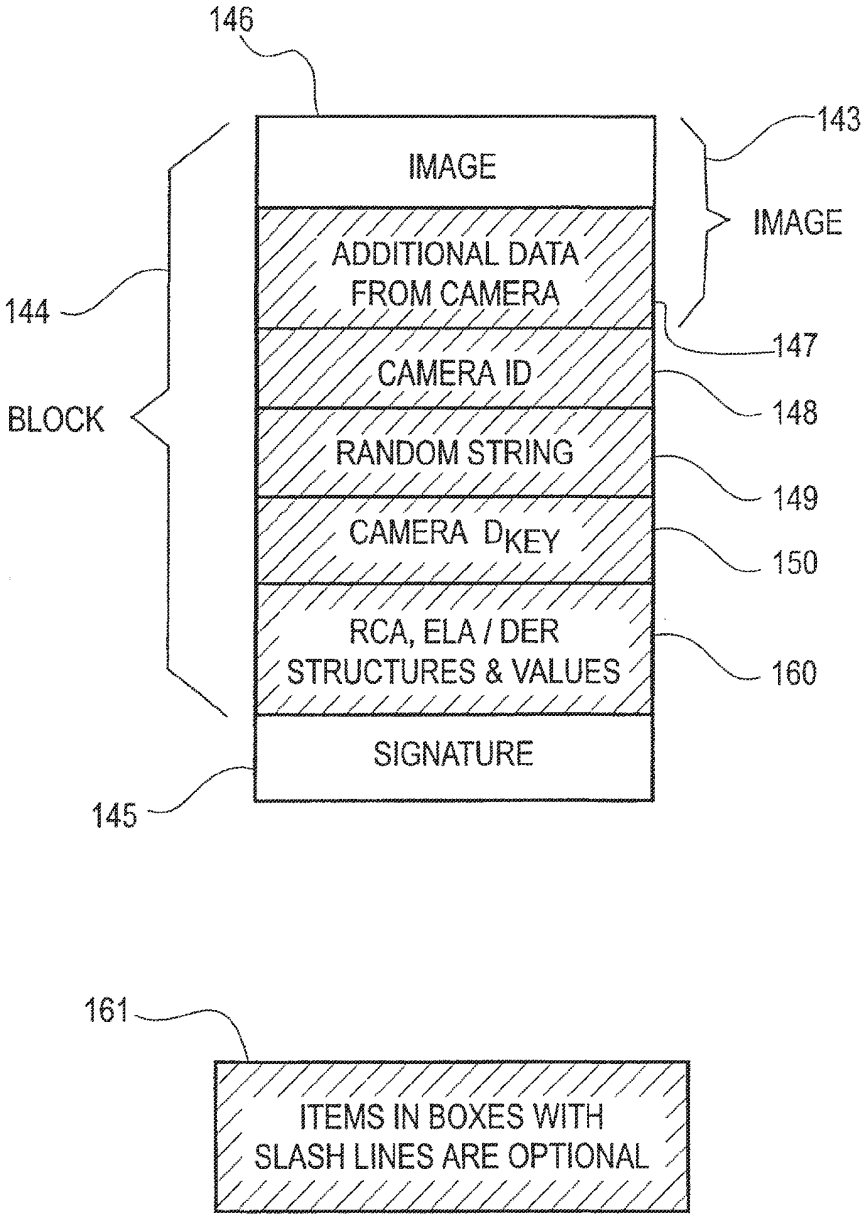

146
143
IMAGE
IMAGE
ADDITIONAL DATA FROM CAMERA
144
147
CAMERA ID
148
BLOCK
RANDOM STRING
149
CAMERA D_{KEY}
150
RCA, ELA / DER STRUCTURES & VALUES
160
SIGNATURE
145
161
ITEMS IN BOXES WITH SLASH LINES ARE OPTIONAL

FIG. 8

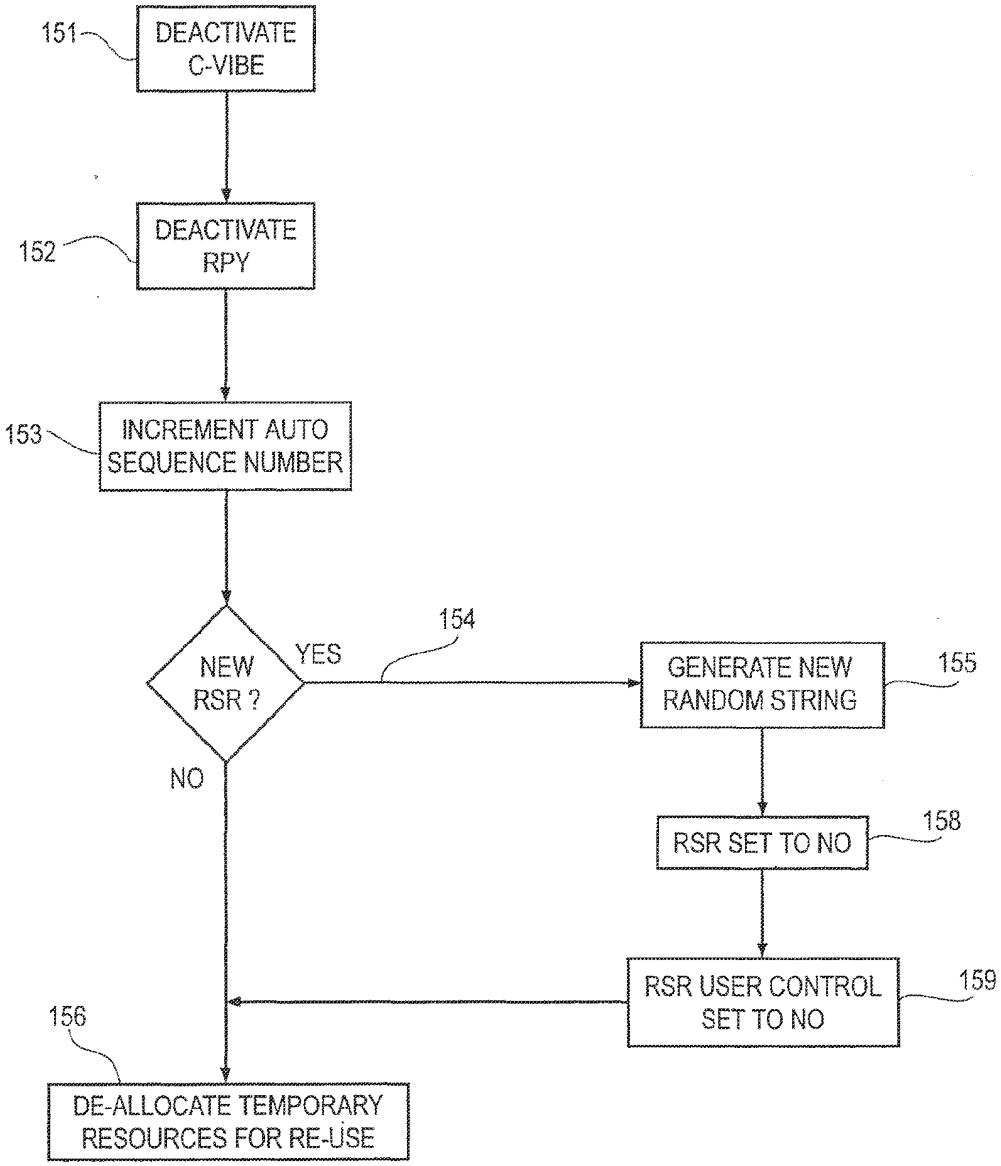
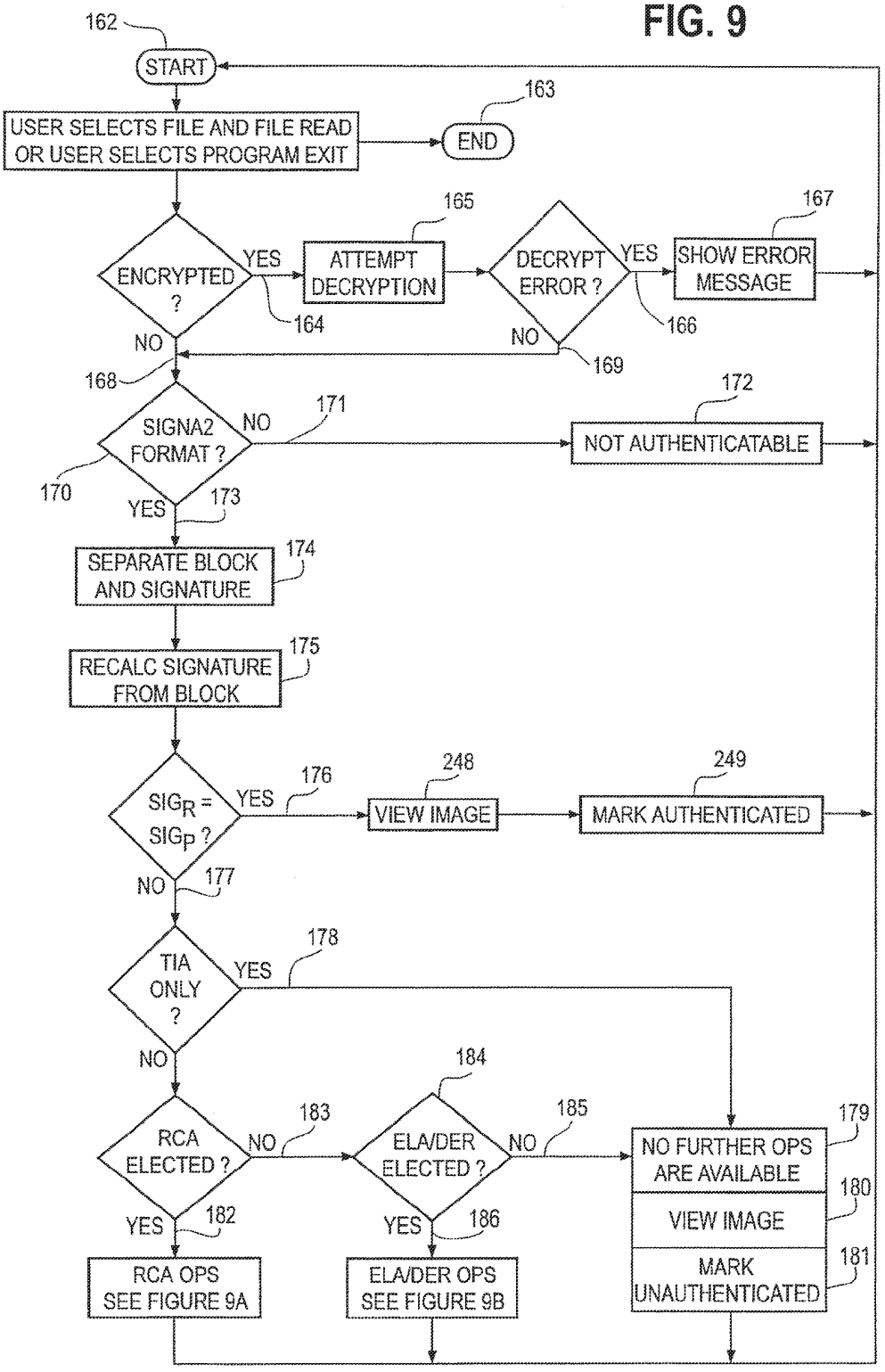

151
DEACTIVATE C-VIBE
152
DEACTIVATE RPY
153
INCREMENT AUTO SEQUENCE NUMBER
NEW RSR ?
YES
154
GENERATE NEW RANDOM STRING
155
NO
RSR SET TO NO
158
RSR USER CONTROL SET TO NO
159
156
DE-ALLOCATE TEMPORARY RESOURCES FOR RE-USE

FIG. 9


162
START
USER SELECTS FILE AND FILE READ OR USER SELECTS PROGRAM EXIT
163
END
ENCRYPTED ?
YES
165
ATTEMPT DECRYPTION
DECRYPT ERROR ?
YES
167
SHOW ERROR MESSAGE
164
166
NO
NO
169
168
SIGNA2 FORMAT ?
NO
171
172
NOT AUTHENTICATABLE
170
YES
173
SEPARATE BLOCK AND SIGNATURE
174
RECALC SIGNATURE FROM BLOCK
175
SIGR = SIGP ?
YES
176
248
VIEW IMAGE
249
MARK AUTHENTICATED
NO
177
TIA ONLY ?
YES
178
NO
184
RCA ELECTED ?
NO
183
ELA/DER ELECTED ?
NO
185
179
NO FURTHER OPS ARE AVAILABLE
180
VIEW IMAGE
181
MARK UNAUTHENTICATED
YES
182
YES
186
RCA OPS SEE FIGURE 9A
ELA/DER OPS SEE FIGURE 9B

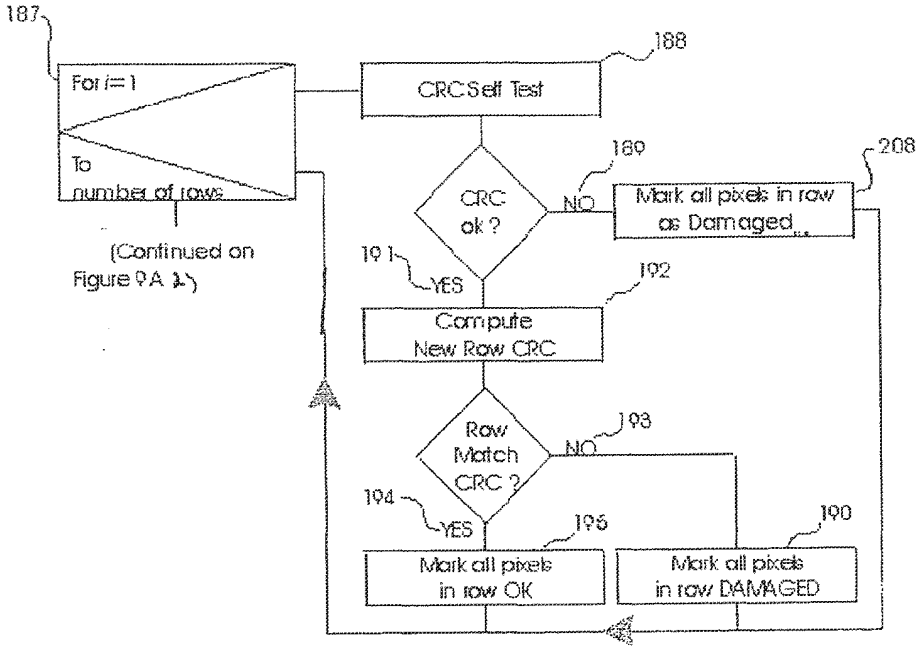

187
For i = 1
To
number of rows
(Continued on
Figure 9A 2)
188
CRC Self Test
189
CRC
ok ?
NO
208
Mark all pixels in row
as Damaged
191
YES
192
Compute
New Row CRC
Row
Match
CRC ?
193
NO
194
YES
195
Mark all pixels
in row OK
190
Mark all pixels
in row DAMAGED

FIGURE 9A

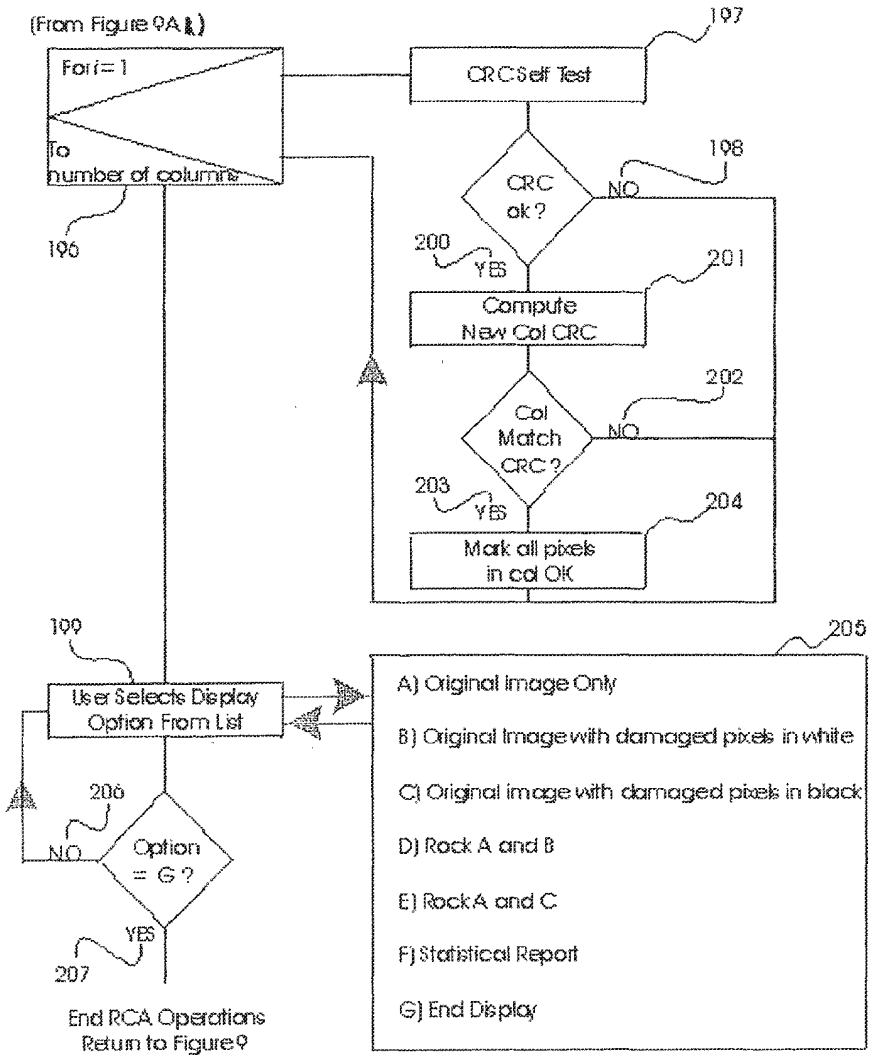

(From Figure 9A1)
For i = 1
To number of columns
196
CRC Self Test
197
CRC ok?
198
NO
200
YES
Compute New Col CRC
201
Col Match CRC?
202
NO
203
YES
Mark all pixels in col OK
204
199
User Selects Display Option From List
205
A) Original Image Only
B) Original Image with damaged pixels in white
C) Original image with damaged pixels in black
D) Rock A and B
E) Rock A and C
F) Statistical Report
G) End Display
206
NO
Option = G ?
YES
207
End RCA Operations
Return to Figure 9

FIGURE 9A2

FIG. 9B-1

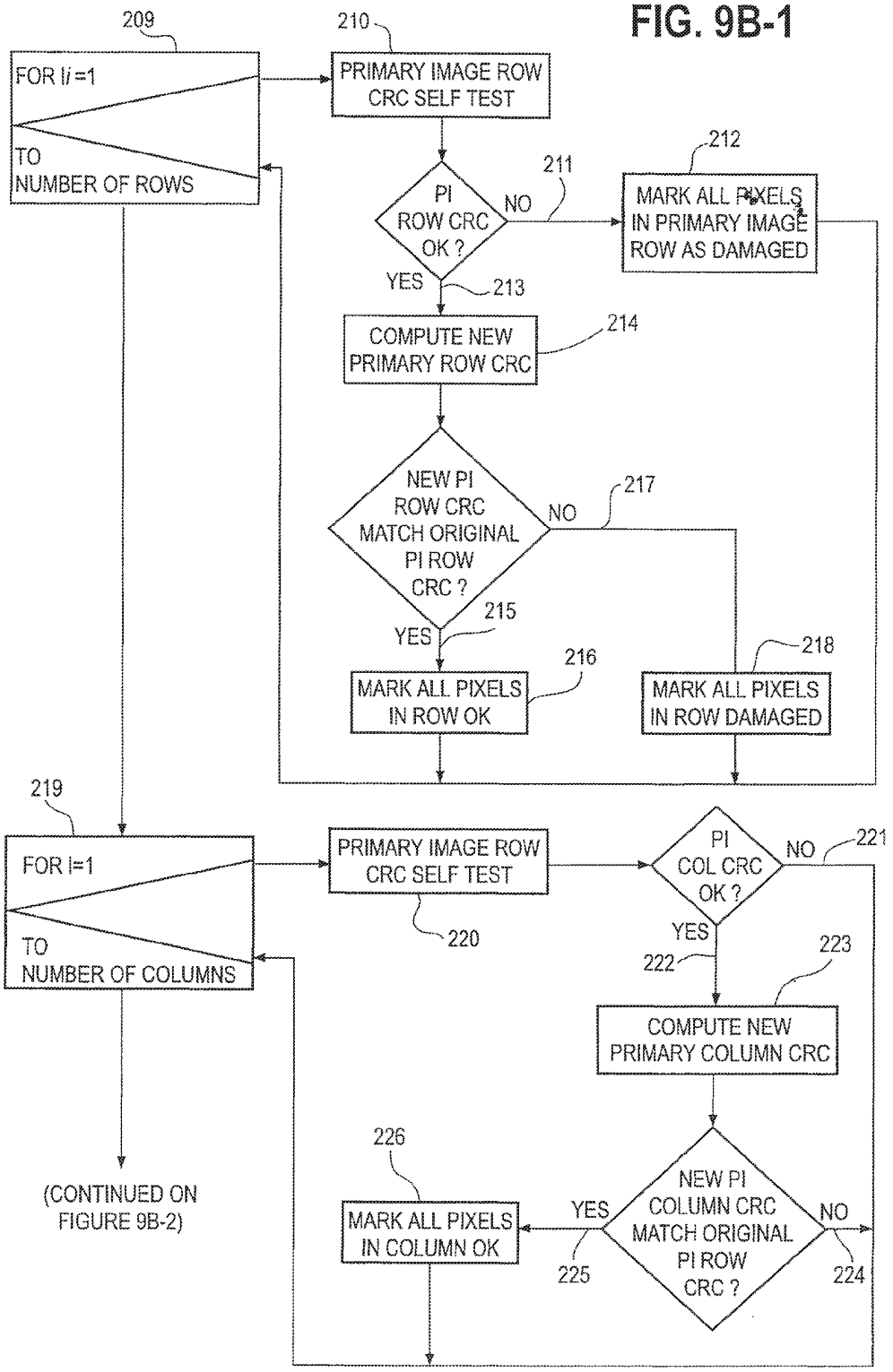
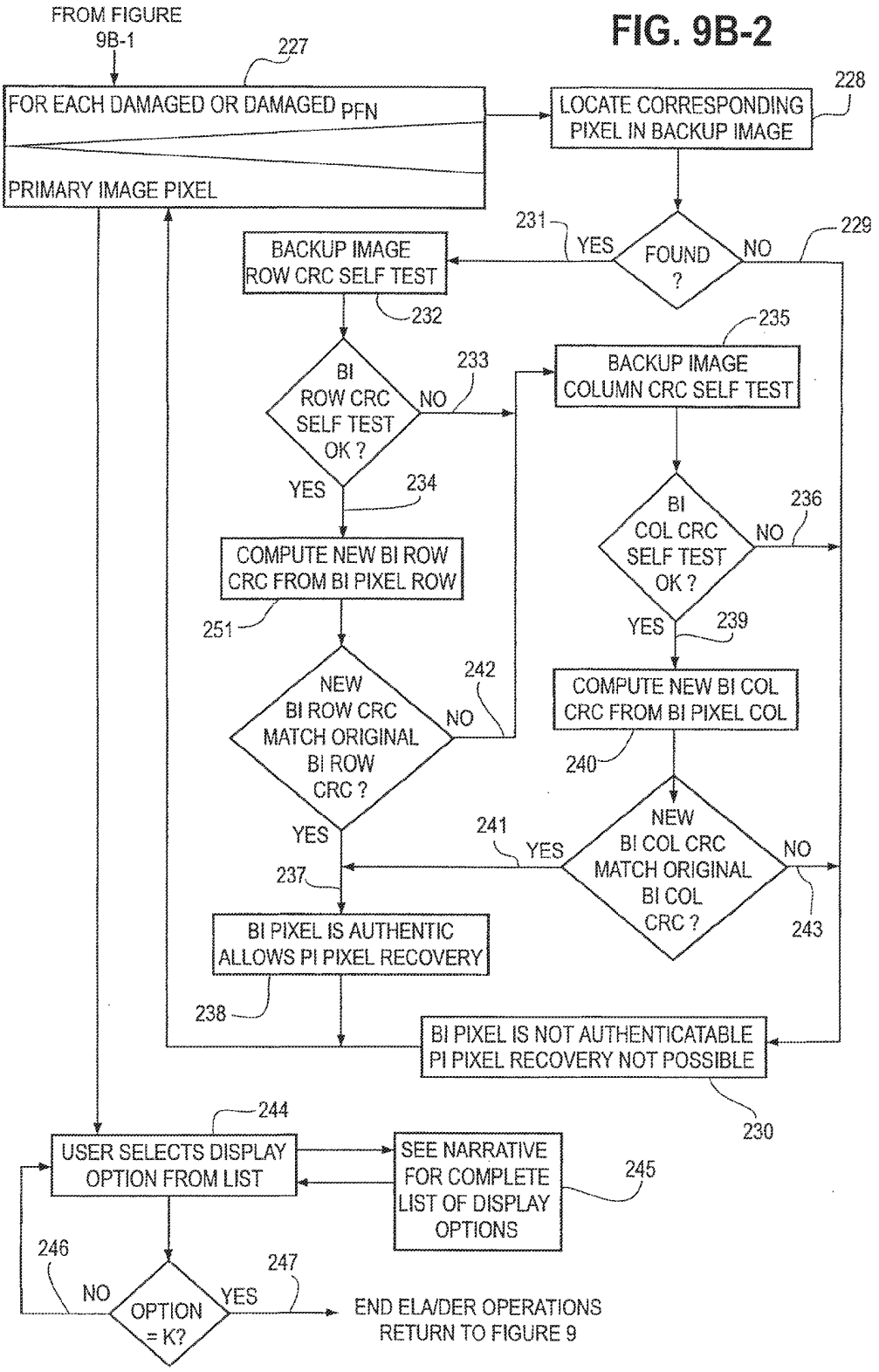

209
FOR I/ =1
TO
NUMBER OF ROWS
210
PRIMARY IMAGE ROW CRC SELF TEST
PI ROW CRC OK ?
NO
211
212
MARK ALL PIXELS IN PRIMARY IMAGE ROW AS DAMAGED
YES
213
COMPUTE NEW PRIMARY ROW CRC
214
NEW PI ROW CRC MATCH ORIGINAL PI ROW CRC ?
NO
217
YES
215
MARK ALL PIXELS IN ROW OK
216
MARK ALL PIXELS IN ROW DAMAGED
218
219
FOR I=1
TO
NUMBER OF COLUMNS
PRIMARY IMAGE ROW CRC SELF TEST
220
PI COL CRC OK ?
NO
221
YES
222
223
COMPUTE NEW PRIMARY COLUMN CRC
226
MARK ALL PIXELS IN COLUMN OK
YES
225
NEW PI COLUMN CRC MATCH ORIGINAL PI ROW CRC ?
NO
224
(CONTINUED ON FIGURE 9B-2)

FIG. 9B-2


FROM FIGURE 9B-1
227
FOR EACH DAMAGED OR DAMAGED PFN
PRIMARY IMAGE PIXEL
228
LOCATE CORRESPONDING PIXEL IN BACKUP IMAGE
231
YES
FOUND ?
NO
229
BACKUP IMAGE ROW CRC SELF TEST
232
BI ROW CRC SELF TEST OK ?
233
NO
YES
234
235
BACKUP IMAGE COLUMN CRC SELF TEST
BI COL CRC SELF TEST OK ?
236
NO
YES
239
COMPUTE NEW BI ROW CRC FROM BI PIXEL ROW
251
COMPUTE NEW BI COL CRC FROM BI PIXEL COL
240
NEW BI ROW CRC MATCH ORIGINAL BI ROW CRC ?
242
NO
YES
241
YES
NEW BI COL CRC MATCH ORIGINAL BI COL CRC ?
NO
243
237
BI PIXEL IS AUTHENTIC ALLOWS PI PIXEL RECOVERY
238
BI PIXEL IS NOT AUTHENTICATABLE PI PIXEL RECOVERY NOT POSSIBLE
230
244
USER SELECTS DISPLAY OPTION FROM LIST
SEE NARRATIVE FOR COMPLETE LIST OF DISPLAY OPTIONS
245
246
NO
OPTION = K?
YES
247
END ELA/DER OPERATIONS RETURN TO FIGURE 9

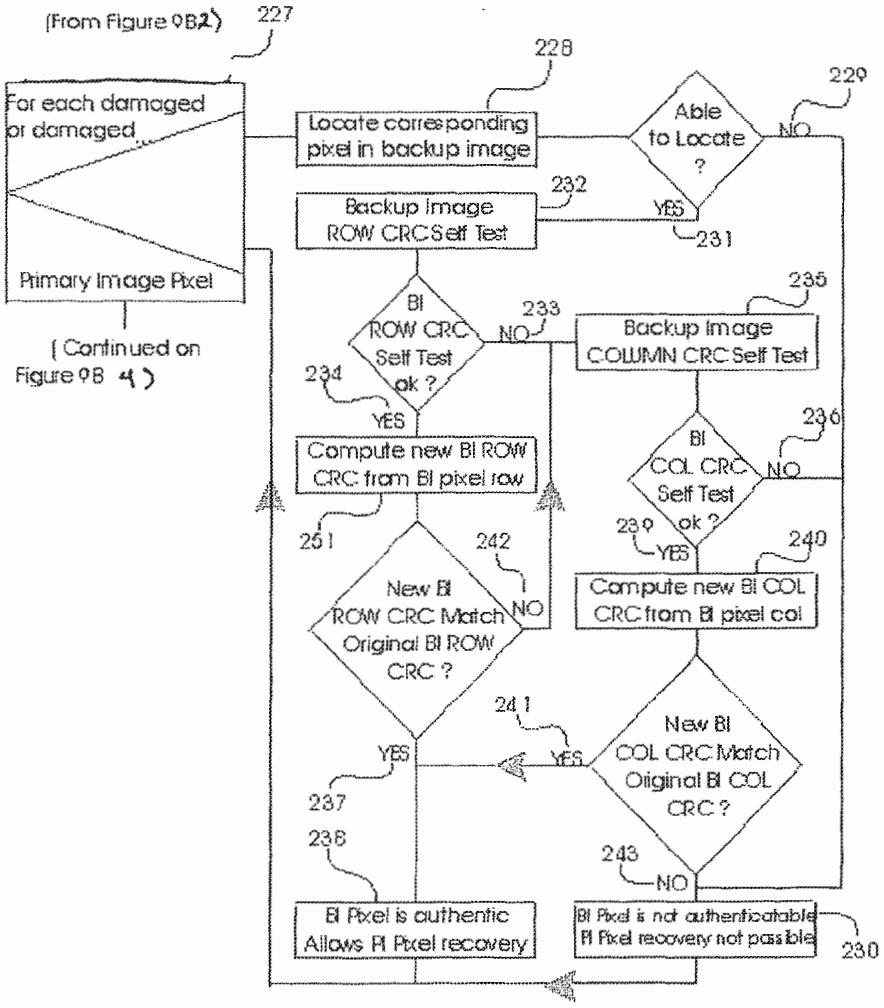

(From Figure 9B2)
227
For each damaged or damaged
Primary Image Pixel
(Continued on Figure 9B 4)
228
Locate corresponding pixel in backup image
229
Able to Locate ?
NO
YES
231
232
Backup Image ROW CRC Self Test
BI ROW CRC Self Test ok ?
233
NO
234
YES
235
Backup Image COLUMN CRC Self Test
BI COL CRC Self Test ok ?
236
NO
239
YES
240
Compute new BI COL CRC from BI pixel col
Compute new BI ROW CRC from BI pixel row
241
242
NO
New BI ROW CRC Match Original BI ROW CRC ?
241
YES
New BI COL CRC Match Original BI COL CRC ?
YES
237
243
NO
238
BI Pixel is authentic Allows PI Pixel recovery
BI Pixel is not authenticatable PI Pixel recovery not possible
230

FIGURE 9B3

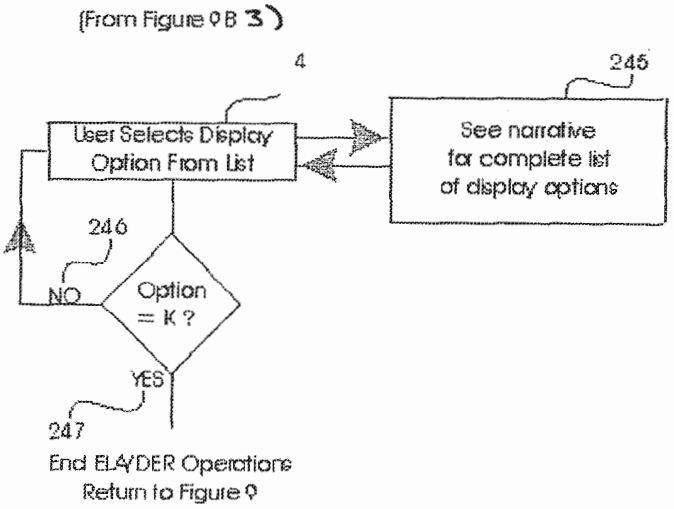

(From Figure 9B 3)
4
245
User Selects Display Option From List
See narrative for complete list of display options
246
NO
Option = K ?
YES
247
End ELAYDER Operations Return to Figure 9

FIGURE 9B4

INDIGENOUS AUTHENTICATION FOR SENSOR-RECORDERS AND OTHER INFORMATION CAPTURE DEVICES

FIELD OF THE INVENTION

The present invention generally relates to a method and apparatus for acquiring and recording a sample of an environment and, more particularly, to a method and apparatus that allows the stored recording to be verified as an authentic, unaltered sample of the environment.

BACKGROUND OF THE INVENTION

One purpose of the present invention is to provide a solution to the problem of either deliberate or inadvertent alteration of recordings. In this context, "recordings" refers to all recordings, including digital images, data files, and the more common audio recording.

Photographs, movies and printed materials have historically been regarded as media that can be trusted to be authentic copies of the original. Early attempts at alteration of photographs for the purposes of revisionist history were almost comically detectable with five people sitting at a table, but six pairs of legs underneath. Hand written, permanently bound, notebooks are used in research laboratories for their resistance against attempts at alteration. Recent technological advances have brought the ability to alter images to the neophyte level. When a master employs the advanced technology the alterations are almost completely undetectable. For this reason digital photography is seldom used in situations when "chain of custody" requirements exist to protect the authenticity of a recording be it photographic, written or auditory. For example, the picture of an accident scene could be altered to show bottles of alcoholic beverages around the driver, even if those bottles hadn't really been there when the picture was taken, but were a post accident embellishment.

A digital camera with apparatus for authentication of images produced from an image file is disclosed in U.S. Pat. No. 5,499,294. Referring to FIG. 3A of U.S. Pat. No. 5,499,294, a block diagram of a system including a digital camera is shown that produces a file image with a digital signature. A device specific decryption key is required to allow a file image to be authenticated. Furthermore, in order to determine whether a file image is authentic, the person performing the authentication must know which camera took the picture; due to the fact that each camera includes a unique private encryption key.

SUMMARY OF THE INVENTION

It is desirable to provide an improved method and system for determining the authenticity of a sample of an environment. A digital signature is created that is a function of both the sample of the environment itself, as well as at least one parameter that is representative of at least one condition under which the digital sample was acquired. The sample is stored in memory together with the at least one parameter and the digital signature. Authenticity of the stored image is determined by creating a new signature from the stored image and at least one parameter, and then comparing the two signatures to determine if they are the same.

Such a method and apparatus is advantageous for several reasons. First, one aspect of the present invention is that it is not necessary to know what device sampled the environment because it only is necessary to have the stored sample, parameters, and signature. Second, encryption is not required for authentication purposes, thereby allowing information storage devices to be manufactured in a more cost effective manner.

Other features and advantages of the present invention will become apparent from the following description.

DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram of one embodiment of the present invention showing a digital camera, a personal computer, and an external GPS unit;

FIG. 2 is a schematic diagram of a self-contained digital camera that incorporates certain aspects of the present invention;

FIG. 2A is a detailed schematic diagram of a self-contained digital camera that incorporates certain aspects of the present invention.;

FIG. 3 is a flow chart of an operational sequence according to a first embodiment of the present invention;

FIG. 4 is a flow chart of the Pre Capture Operations from FIG. 3;

FIG. 4A1 is a flow chart of the Check Additional Inputs for Pre Capture Operations in FIG. 4;

FIG. 4A2 is a continuation of the flow chart from FIG. 4A1;

FIG. 4B is a flow chart for recording the user controls during the Pre Capture Operation;

FIG. 5 is a flow chart of the Capture Operations from FIG. 3;.

FIG. 6 is a flow chart of the Post Capture Operations from FIG. 3;

FIG. 6B is the continuation of the flow chart from FIG. 6;

FIG. 7 is a flow chart of the Recording operation from FIG. 3;

FIG. 7A is a diagram of a file format for a signed digital image.

FIG. 8 is a flow chart of the Clean up and Preparation from FIG. 3;

FIG. 9 is a flow chart of the Authentication Sequence;

FIG. 9A1 is a flow chart of the RCA Operations from FIG. 9;

FIG. 9A2 is a continuation of the flow chart from FIG. 9A1;

FIG. 9B1 is a flow chart of the ELA/DER Operations from FIG. 9;

FIG. 9B2 is a continuation of the flow chart from FIG. 9B1;

FIG. 9B3 is a continuation of the flow chart from FIG. 9B2;

FIG. 9B4 is a continuation of the flow chart from FIG. 9B3;

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

One aspect of the present invention is the concept and method of indigenous authentication. That is, a family of devices to create recordings with material to validate its authenticity. One embodiment of the present invention relates to digital photography where an image is authenticated as a whole. An intermediate version allows the authentication of less than the whole. An advanced version allows for recovery of damaged (altered from its original state) elements. Additional inputs including, but not limited to,

date, time, latitude, longitude, altitude, roll, pitch, yaw, and compass heading can be made part of the image as well as the status of camera elements including camera identification, image sequence number, flash status, lens zoom factor, counter vibration status, focus status and focus quality. This additional information becomes part of the recording and can also be authenticated.

The present invention is applicable to information capture scenarios other than digital cameras such as self-authenticating identification documents, an extension of the notary public system, or electronic laboratory notebooks to replace the handwritten ones mentioned above. Once established as a trustworthy source; the indigenous authentication concept can be extended further for recording quality control, legal requirements and financial instruments.

A key to verifiable authenticity is to insure that the authentication information generation is tightly coupled to the sensor set and recorder. There can be nothing that can possibly alter the recording before the authentication information is generated. Authentication using this method requires neither comparison files, nor conventional or reverse encryption. The strength of authentication is increased by using one-time random elements and by the use of a random string, regenerated under user control. Although not required for basic operation, the resulting recording can be optionally encrypted to conceal the information. The absence of required conventional encryption or reverse encryption eliminates the need for a public registrar or record keeping relating to the management of decryption keys. As the authentication is indigenous there is no requirement to identify which recorder was used.

Referring to FIG. **2**, an environment **2** can be sampled **1** in a variety of formats. In recording a single sample of a visual environment, a single frame optical recorder, generally known as a camera, is used. The sample taken, known as a "photograph," has been recorded on positive transparency films (slides); negative transparency films (negatives); opaque or translucent prints; and more recently as digital files.

In recording a continuous sample of a visual environment, a continuous optical recorder such as a video camera, movie film camera or a digital movie camera is used. These samples, generically called "movies," have been recorded on transparency film, videotape and more recently as digital files

In recording a sample of an auditory environment, a continuous audio recorder such as a tape recorder or a digital recorder is used. These samples, generally called "recordings," have been recorded on a wide variety of wire, tape and digital files.

With the development of sensors and recorders, the recording of samples of taste, touch and smell can be accommodated in the same generic model. Also, samples are not limited to the five human senses. The method for authentication and verification disclosed in the present application can be used on samples taken from any sensor set including, but not limited to, the full range of physical, chemical, and spectral phenomena.

To ensure authentication, additional inputs **7** other than the sensor set **4** are not accessible to the user without detection as shown in FIG. **2**. To accomplish this the additional inputs are shown inside the device physical boundary Analog recorders may also be incorporated into this system through the use of analog to digital converters.

One use of the present invention is to create an image or data file that is considered "trustworthy" in any situation where proof of authenticity is necessary. This includes, but is not limited to, legal evidence, insurance claims, project management, scientific research, invention, quality control, identification, intelligence gathering, purchasing, command and control, law enforcement, document and image transmission.

The increasingly rapid transition to digital capture, analysis, storage, transmission, distribution and use of information, using increasingly sophisticated hardware and software for creation and capture tools, makes it increasingly difficult to accept any image or data file as authentic on its face.

With the continued growth of personal computers in society and the increasing use of the internet, electronic miscreance including deliberate fraud and inadvertent changes caused by transmission or storage errors are on the rise. The need for authentication parallels that rise to counter proliferation of altered files. The need for authentication also increases with the potential damage an altered file might cause. For example, contracts, purchase orders, legal decisions, electronic bill payments, electronic invoices, quality control information, blue prints, designs: all of these could cause great harm if an altered version were believed to be authentic. It is not unreasonable to presume that indigenous authentication might become the norm, in an attempt to prevent or derail any possible malicious acts by miscreants.

One aspect of the present invention allows generally complete mitigation of the threat of undetected image alteration and subsequent use of the altered image for purposes of deliberate or unknowing deception. Thus, a framework is provided for future devices to accomplish similar ends and provide a solution to an ever more troubling social and economic problem, namely the eroding credibility of photographic images, especially in law enforcement where the images may become evidence in a legal proceeding.

Referring to FIG. **1**, a schematic diagram of one embodiment of the present invention showing a digital camera, a personal computer, and an external GPS unit is shown. A general purpose microcomputer **252** is used to simulate the processor **157** and its programming. The mouse **256** and keyboard **257** are used to simulate the user's setting of controls (See FIGS. 2A, **9 10 11 12 13**). The microcomputer's monitor **253** is analogous to the process monitor **8** shown in FIG. 2A. An external geographic positioning system **254** (GPS) is used instead of an internal **44** one. An externally connected digital camera **255** simulates the lens sensor set **73** auto focus **19** and flash generator **30**. The microcomputer's **252** floppy drive (not shown) performs the function of the recorder **142** and the 3.5" floppy disk **259** is the removable storage media **141**.

Referring to FIG. 2A, a device model for a single frame optical recorder, more commonly known as a camera, is shown. FIG. 2A does not show the externally supplied source or internal batteries that must power this device. In this camera, the user may access the process monitor **8**. For approximate aiming, access may be gained through a shaft, parallel to the axis of the lens. Access to the process monitor **8** may also be gained through a processor **157** controlled recreation of the current scene. Indicators appear on the process monitor indicating flash status, zoom status, etc.

Operators may aim the device, activate the device, and set user controls, including but not limited to, flash **9** zoom **10** random string recording (RSR) **11** or optional encryption **12**. During the operation of the camera, internal security **14** is monitored to detect the integrity of the tight coupling of the sensor set and the recorder **6**.

Referring to FIG. 3, when the processor 157 receives an activation signal, the multi phase operating cycle proceeds through the pre capture, capture, post capture, recording, clean up and preparation operations before returning to the pre capture phase. To reduce the time within each phase, parallel processing and other engineering techniques are used.

Referring to FIG. 4, the pre capture sequence is the most common operating phase of the unit. The device cycles in the pre capture operation 65 until activated by user control 13 or turned off 15 in preparation for normal termination 95. If the device is turned on and inadequate 16 power is present to complete the operating cycle, the user activation will have no effect. An indication 17 is given to the user through the process monitor and no further processing is completed 66.

If sufficient power is present to complete the operating cycle, the additional inputs and components are checked. Referring to FIG. 4A 1 the auto focus 19 sensor and processor are then checked 20. If a malfunction 21 is present the process monitor 8 will be updated with an error message 22 to inform the user.

Independent of the auto focus's status, processing continues checking the focus quality sensor 23 the flash generator 30 counter vibration unit (C-VIBE) 35 and the roll, pitch, yaw (RPY) unit 40. These tests are performed in order (20, 25, 29, 34 and 39) independent of resulting status. At each stage, if a malfunction is present, the process monitor is updated with an error message to inform the user (27, 32, 37 and 250).

Referring to FIG. 4A2 the status processing continues 42 with a check 43 of the global position system (GPS) unit 44. If there is a malfunction 45 the value "NO GPS" is recorded 46. If no malfunctions 47 are present, the current GPS coordinates and other GPS information are recorded 48 and the process monitor 8 is updated 49 with an error message or the current coordinates.

Independent of the GPS status, processing continues 50 with a check 51 of the internal compass 52 If a malfunction 53 is present, the value "NO COMPASS" is recorded 54. Otherwise 55 the current compass heading is recorded 56 and the process monitor 8 is updated 57 with an error message or the current heading.

Independent of the compass status, processing continues 58 with a check 59 of the internal security system 14. If there is a breach of security 60 the violation is recorded 61. Otherwise 62 the value "ImageGuard" is recorded 63 and the process monitor 8 is updated 64 with the violation or "ImageGuard"

Referring to FIG. 4, after the additional inputs and components are checked 18 the user control modifications are recorded 67. Referring to FIG. 4B, the current setting for the flash generator 30 is checked 68 against the flash settings 9 provided by the user. If not identical 69 the setting for the flash generator 30 is set 70 to that provided by the user.

The user's zoom setting 10 is then checked 72 against the zoom setting of the lens 73. If not identical 74 the setting for zoom 73 is set 75 to that provided by the user. The current random string record (RSR) value is then checked 77 against the setting 11 provided by the user. If not identical 78 the RSR value is set 79 to that provided by the user. The two possible values are "Y" for "Yes, record a new random string with the next image" and "N" for "No, don't record a new random string with the next image."

The current encryption value is then checked 81 against the encryption value 12 provided by the user. If not identical 82 the current encryption value is set 83 to that provided by the user. The three possible values are "Y" for "Yes, produce an encrypted image only", "N" for "No, don't produce an encrypted image, produce an unencrypted image only" and "B" for "Produce both an encrypted image and an unencrypted image." During this process the process monitor. 8 is updated 85 to reflect any changes made.

Referring to FIG. 4, once the user control modifications are recorded 67 processing continues 86 with a test 87 for adequate recording media. If there is inadequate recording media 88 the process monitor 8 is updated 89 with an error message and no further processing is completed 90 past this point.

After the test dealing with adequate recording media is completed 91 all pre capture operations are complete. A test 92 is made for the status of the activation control 13. If the control is not active 93 processing is cycled 65 and if active, processing continues 94 with capture operations.

Referring to FIG. 5, once the user activation control 13 is active, processing moves from pre capture operations (see FIG. 4) to capture operations.:(see FIG. 5) Current values are acquired 96 from the GPS and:Compass system. If the GPS is not, active 45 the "NO GPS" value 46 is recorded. If the GPS is active 47 the GPS coordinates 48 are recorded as is the current date and time. If the Compass, is active 55 the current heading is recorded and if not active 51, the "NO COMPASS" value 54 is acquired.

At this point, if required 97 the counter vibration unit (C-VIBE) is activated 98 to counter vibration. The roll, pitch and yaw (RPY) sensors are activated 99 and the need to prime 105 the flash unit is determined. A test is made for the user commanding the flash on or off 100. If the flash is commanded on 101 or auto flash detects 103 the requirement 104 for a flash, the flash is primed 105 and the image is captured with flash 108. Otherwise the image is captured without a flash 107.

Focus quality points are detected 109 by accessing the focus quality additional input 23. The number of focus quality points is selected, and the maximum range and minimum range are recorded. Here the camera uses either sound ranging, or another technology to measure depth of field. This procedure is required for auto focus and would detect the reproduction of a picture. This procedure also reports the number of points with differing ranges as well as the closest and farthest focus quality points from the camera. For example, "10 p 1 m Inf" would mean 10 points of differing depth, the nearest being one meter, the farthest is infinity.

Referring to FIG. 6, once the image has been captured (see FIG. 5) processing moves to post capture operations. First the CCD (or other sensor) is polled 110 to gather the image and pre pare it for recording. The GPS values for latitude, longitude, altitude, date, time, and satellites used for the positioning; that were previously acquired 96 are then appended 111 to the image. If the GPS was not functional 45 the "NO GPS" value 46 is appended 111 to the image. The AutoFocus status; number of focus quality points 109; maximum range and minimum range; flash value (commanded on, commanded off, auto-flash required, or auto-flash not required); counter vibration value (active 98 or not); roll, pitch and yaw (RPY) values; recorded compass heading 96; lens 73 zoom setting; camera identifier (CamID 124 set by the factory and unalterable by the user); current image sequence number 125; current random string 126; and file type (127 set by the factory and unalterable by the user) are all appended to the image. If internal security is compromised 60 a security violation 61 is appended 123 to the image. Otherwise the "ImageGuard" value is appended 123 to the image.

Referring to FIG. **6B**, there are three levels of authentication and damaged element recovery. The initial level is total image authentication (TIA). At this level only the entire image is authenticated or not. The second level is row/column authentication (RCA) where each row and column of the picture elements (pixels) can be authenticated independently. Under RCA, less than the whole image can be authenticated. The third level is elemental level authentication (ELA) and damaged element recovery (DER).

Under the ELA structure, each and every single pixel can be authenticated independently. If a single pixel fails authentication (damaged) there are structures added to the image in the post capture operation which provide multiple methods of determining the original value of the damaged pixel. This is called damaged element recovery (DER). Initially the level of authentication and damaged element recovery is to be set at the factory so that no affiliated user control (**9**, **10**, **11**, **12** and **13**) is shown. There can be only one level of authentication (TIA, RCA, ELA/DER) active per use. (See FIG. **9** "Authentication Sequence" and more on authentication.)

If RCA is elected **128** the RCA structures and values are computed and appended **129** to the image. If ELA/DER is elected **130** the ELA/DER structures and values are computed and appended **131** to the image. The signature protocol used in - this device is the commercially available MD5 but the signature protocol is not limited to the MD5. The digital signature **132** which is a function of the signature protocol (SP) being used and the block, is computed and made part of the file. (SIGNA=*f* (SP (Block))) The Block **144** is the digital data composed of the image and optionally: additional information, the camera id, the random string, the camera decryption key, and the RCA and ELA/DER structures and values.

If the user has elected **133** no encryption, or both encrypted and unencrypted, as set by the user control **12** and evidenced by the encryption value **83** then an unencrypted version of the complete image file is created **134**. If the user has elected **135** encryption, or both encrypted and unencrypted, as set by the user control **12** and evidenced by the encryption value **83** then an encrypted version of the complete image file is created **136**.

Referring to FIG. **7**, if the user has elected **137** no encryption, or both encrypted and unencrypted, as set by the user control **12** and evidenced by the encryption value **83** then an unencrypted version of the complete image file is written **138** by the recorder **142** on the recording media **141**. If the user has elected **139** encryption, or both encrypted and unencrypted, as set by the user control **12** and evidenced by the encryption value **83** then an encrypted version of the complete image file is written **140** by the recorder **142** on the recording media **141**.

Referring to FIG. **2A**, a 3.5" floppy drive **142** and removable 3.5" floppy diskette **141** is shown as the recorder and recording media. Other available recording options include flash RAM with removable memory modules, and storage not internal to the device via infra red, serial, Ethernet, Token Ring, parallel, universal serial bus (USB), firewire or other communication mode to either a single computer or a network of computers.

Referring to FIG. **7A**, the files created by the Signa2 process are in a format generally accepted by the industry. Most specifically, the Signa2 files are not proprietary. Additional information is contained within the file, but the addition of the information is in compliance with the standards for the format.

There are two braces in the figure. The first titled "Image" indicates the two elements that are viewable by programs compliant with generally accepted industry formats. Elements outside this brace are not viewable by programs compliant with generally accepted industry formats. The second **144** titled "Block" indicates the elements covered by the signature **145**. Everything inside the "Block" is what is signed.

Elements shaded in gray **161** are optional and not required to fulfill the basic purpose of Signa2 devices. A tightly coupled image **146** and signature **145** are the minimum required elements for the Signa2 process. The sensor set **73** acquires the image **146** which is the minimum viewable information. Additional data from the camera **147**, viewable by the user, include: Global Positioning System (GPS) information **111**; zoom settings; AutoFocus status; the results of the focus quality sampling; roll, pitch and yaw (RPY) values; the compass heading; flash status; File Type; CamID; Seq **120**; and Security Value.

The GPS information **111** may include **48** latitude, longitude, altitude, date, time, satellites used in the determination or "NO GPS" **46** if there is a fault **45** with the system. The zoom setting **75** information includes the setting used by the lens **73** for capturing the image expressed either in millimeters with 50 mm being "eye-normal", or in X where 1X is 50 mm. The compass heading **117** includes information on which way the camera was pointing at the time the image was captured.

The flash status **114** information includes the commands, Commanded ON, Commanded OFF, Auto ON or Auto OFF. In the flash status, the first two refer to settings forced by the user and the latter two refer to the user allowing the camera to decide to flash or not and whether it did or not. There may be other options.

The CamId **119** or camera identification code, is set at the factory and part of each image. Examples are SHEP0001 or MOLL0454. Although not required for authentication it does provide a means of determining, at least initial ownership of the device.

Seq **120** is the sequence number for unique image identification, automatically incremented. When used with CamId above BECK5102-98312 uniquely identifies the camera and the picture.

The two Security Values **123** are ImageGuard and NONVERIFIED. ImageGuard appears if no internal errors are detected and the security is not compromised. NONVERIFIED (or other indication of compromise) appears if security is compromised within the system.

Other segments within the File Structure include Camera ID **148**; Random String **149**; Camera Decryption Key **150**; RCA and ELA/DER structures and values **160**; and the digital signature **145**. The Camera ID **148** is the unique camera identification, the same as above, but in a section of the file not viewable by the user. The Random String **149** is the current random string and is made part of the file. The Camera Decryption Key **150** is a camera specific decryption key that stays in the camera.

Referring to FIG. **8**, this figure illustrates the process for clean up and preparation. In this portion of the process, functions not useful in pre capture operations (see FIG. **4**) are deactivated and preparations are made for subsequent image capture. The counter vibration, and the roll, pitch, yaw are deactivated **151**, **152** and the image sequence number is incremented **153**.

If the "Random String Recording" has been set **79** to YES by the user control **11** the image itself and other information

(Referring to FIG. 7A) are used to generate **155** a new random string that replaces the previous random string. The "Random String Recording" **79** is then reset **158** to NO and the user control **11** is set **159** to NO. Temporary resources used by the processor **157** are then deallocated **156** to prepare them for re-use.

It is important to note that the previous random string is used for the image just created. Therefore, frequent resetting of the random string will deter pattern recognition and increase security. This is discussed in the "Role of the random string in increasing the strength of the digital signature" below.

Referring to FIG. **9**, authentication starts with a file believed to contain an image and the additional items (see FIG. 7A) to make the file authenticatable as a Signa2 image. The authentication program must be easily and freely available from a secure public source. Otherwise someone seeking to deceive could provide a faux-authentication program to generate a forced-negative or forced-positive authentication.

The program starts **162** with a self diagnostic to insure that the authentication program itself has not been damaged or corrupted. This self diagnostic is repeated each time processing reaches this **162** point to guard against alterations made after the program has been loaded. Should the self diagnostic fail the program immediately ends with an error message. This self diagnostic procedure and the possibility of a failure are not shown on FIG. **9**.

Once the authentication program has been loaded the user is presented with an opportunity to select a file or elect program exit. If the user elects program exit the authentication program ends **163**. If an encrypted file is selected **164** an attempt **165** is made to decrypt the file This may require a decryption key obtained from the user or taken from-the file **150**. If a decryption error **166** occurs, an error message **167** is displayed and the program cycles back to start **162**

If the file was not **168** encrypted or was decrypted without error **169** a test **170** is made to confirm that the file is in the Signa2 format. If the file is not **171** in Signa2 format, the file is not authenticatable **172** and the program cycles back to start **162**

If the file is **173** in Signa2 format ,the block **144** is separated **174** from the signature **145** and the signature is recalculated **175** from the original block **144**. If the recalculated signature (SIG_R) matches **176** the provided signature (SIG_P), the image may be viewed **248** and is marked authenticated **249** as a valid image using total image authentication (TIA). The program then cycles back to start **162**.

If the two signatures do not match, and the authenticator program has been acquired from a trusted source and is free from alteration; then the image file has been damaged or altered. This is a true-negative, an image properly determined not to be authentic. With an uncompromised authenticator program, a Signa2 image file using TIA level authentication cannot generate false-negatives. The image and the signature are in a single file and altering the file, either intentionally or accidentally; constitutes invalidation and a proper negative authentication.

If the recalculated signature (SIG_R) does not **177** match the provided signature (SIG_P), a series of tests are made for one of three authentication levels. If only total image authentication (TIA) is available **178** then no further operations are available **179**. The image is viewed **180** and marked unauthenticated **181**. The program then cycles back to start **162**.

Referring to FIG. **9**, if row/column authentication (RCA) is **182** elected, processing continues with RCA Operations and the program cycles back to start **162**. If row/column authentication (RCA) has not **183** been elected, a **184** test for elemental level authentication/damaged element recovery (ELA/DER) is made.

Referring to FIG. **9B1** if ELA/DER has **186** been elected, processing continues with ELA/DER Operations and the program cycles back to start **162**. If ELA/DER has not been elected **185** there is an error condition as one of the three levels of authentication (TIA, RCA, ELA/DER) should be available. This error condition is handled by reporting no further operations are available **179**. The image is viewed **180** marked unauthenticated **181** and the program cycles back to start **162**.

Referring to FIG. **9**, row/column authentication (RCA) is elected **182** when a file in a Signa2 format **173** has a signature failure **177**. The signature used in comparison **145** is a single signature for the entire file. RCA structures and values **160** provide for a method of detecting errors, not at the whole file level, but at a level for each row and column. Checking each row and column provides two opportunities to detect an error for each pixel.

Cyclic Redundancy Check (CRC) is the method used to describe this form of error detection. There are several varieties of CRC as well as other algorithms for error detection of this type. Although CRC is used here for description purposes, other error detection codes (or error correction codes such as Hamming and Reed-Soloman) may be implemented to augment or replace the CRC error detection code.

Referring to FIG. **9A1** a digital image consists of picture elements, known as pixels, arranged in a matrix of rows and columns. RCA Operations commence by stepping **187** through each row of the image testing **188** the CRC for internal integrity. Although CRCs do not contain an inherent internal integrity test, part of the RCA structures include additional values to test the CRC. If the CRC fails **189** this self test, all pixels in that row are marked as damaged, but potentially false negatives (PFN) **208**.

If the CRC itself is ok **191** the entire row of pixels is used to compute **192** a new CRC for the row. This new CRC is compared to the original CRC. If they do not **193** match, all of the pixels in the row are marked as damaged **190**. If the new CRC does **194** match the original CRC, all of the pixels in the row are marked **195** ok.

Referring to FIG. **9A2** RCA operations continue by stepping **196** through each column of the image and testing **197** the CRC of each column for internal integrity. If the CRC fails **198** this test, no further operations are conducted on the column of pixels. If the CRC itself is ok **200** the entire column of pixels is used to compute **201** a new CRC for the column. If the new CRC does not **202** match the original CRC, no further operations are conducted on this column. If the new CRC does **203** match the original CRC, all of the pixels in the column are marked **204** ok.

A pixel may be marked in one of six ways: Ok—ok from row CRC **195** and column CRC **204**; Damaged—ok from row CRC **190** and column CRC **204**; $Damaged_{PFN}$—ok from row CRC failure **189** **208** and column CRC **204**; Ok—null from row CRC **195**; Damaged—null from row CRC **190**; and $Damaged_{PFN}$—null from row CRC failure **208**. There is no second status because of column CRC failure **202**.

The nature of the two operations (row and column) generate a matrix where some rows of pixels may be marked as damaged in the row operations and some of those pixels changed from damaged to ok by the column operations. This

is because an entire row is marked damaged or ok. If a column is marked ok, the pixels that may have been marked damaged as part of a whole row were not in fact damaged and are changed to being ok. As an example, a single damaged pixel would cause a whole row to be marked as damaged in row operations. Column operations would mark every column ok except the column that had the damaged pixel. The end result is an image with a single pixel marked damaged.

Once the image has been authenticated the user selects **199** from a list of presented display options **205**. The display options are: Option A—Display only the original image without any modification; Option B—Display the original image with damaged pixels forced to white; Option C—Display the original image with damaged pixels forced to black; Option D—Rock A and B; Option E—Rock A and C; Option F —Statistical Report; and Option G—End display options. "Rocking" refers to rapidly displaying two alternating images.

The statistical report under Option F contains the following elements: F1 contains the total number of pixels in the image. F2 contains the total number of pixels marked ok—ok, Damaged—ok, Damaged$_{PFN}$—ok and ok—null, expressed as a number, and as a relative percent of the total number of pixels (F2/F1)*100 known as the "Undamaged Percentage."

Ok—ok pixels passed both row **194** and column **203** CRC test. Ok—null pixels passed the row **194** CRC test, but the column CRC was damaged **198** and provided no additional information. Damaged—ok pixels were not actually damaged. The pixels were marked damaged because the new row CRC did not match **193** the original row CRC, and the whole row was marked **190** damaged even though the pixels passed **203** the column CRC test Damaged$_{PFN}$—ok also contains pixels that were not actually damaged. The pixels were marked damaged due to the row CRC failure **189** that caused the entire row to be marked Damaged$_{PFN}$ even though the pixels passed **203** the column CRC test.

F3 contains the total number of pixels marked Damaged—null expressed as a number, and as a relative percent of the total number of pixels in the image (F3/F1) *100 known as the "True Negative Percentage." The pixels were marked Damaged-null because the new row CRC did not match the original row CRC test **193**. There is no second status because of column CRC failure **202**.

F4 contains the total number of pixels marked Damaged$_{PFN}$—null expressed as a number, and as a relative percent of the total number of pixels in the image (F4/F1) *100 known as the "Potential False Negative Percentage." The pixels were marked Damaged$_{PFN}$—null because the row CRC failed **189** **208** the self test and the pixel could not be authenticated as ok due to column CRC failure **202**. The sum of the relative percents of F2 F3 and F4 should equal 100%, and the sum of F2 F3 and F4 should equal F1.

The user may continue to select **206** alternate display options until they elect to end display options **207**. At that point RCA operations are concluded.

Referring to FIG. **9B1**, ELA/DER Operations occur when a file in Signa2 format **173** has a signature failure **177** and both element level authentication (ELA) and damaged element recovery (DER) authentication are elected **186**. The signature used in comparison **145** is a single signature for the entire file. ELA/DER structures and values **160** provide for a method of determining authentication, not at the whole file level, but at a level for each element.

The ELA/DER structure includes a complete duplicate of the image, compressed and encoded. It is this duplicate image that allows for elemental level authentication and damaged element recovery. In the description below the original version of the image, the one the user can see, is referred to as the "Primary Image", abbreviated PI. The compressed and encoded version of the image is referred to as the "Backup Image", abbreviated BI. Both the Primary Image and the Backup Image have row and column CRCs, or other error detection protocols.

Referring to FIG. **9B1** initially each row **209** of the primary image (PI) is stepped through and a self test **210** is performed on each primary image row CRC. If the CRC fails **211**the self test, all of the pixels in the primary image row are marked **212** Damaged$_{PFN}$ as potential false negative damaged pixels. If the primary image row CRC passes **213** the self test, a new primary row CRC is computed **214** from the pixels in the primary image row. If the new primary image row CRC matches **215** the original primary row CRC, all the pixels in the row are marked **216** as ok (undamaged). If the new primary image row CRC does not **217** match the original primary row CRC, all the pixels in the row are marked **218** as damaged.

Referring to FIG. **9B2**, once the row-wise process is complete, each column **219** of the primary image is stepped through with a self test **220** performed on the primary image column CRC. If the CRC fails the self test **221** no further operations are conducted on this column. If the primary image column CRC passes **222** the self test, a new primary column CRC is computed **223** from the pixels in the primary image column. If the new primary image column CRC matches **225** the original primary image column CRC, all of the pixels in that column are marked **226** ok. If the new primary image column CRC does not **224** match the original primary image column CRC, no further operations are conducted on this column.

Each pixel may be marked in one of six ways: Ok—ok from row CRC **216** and column CRC **226**; Damaged—ok from,row CRC **218** and column CRC **226**; Damaged$_{PFN}$—ok from row CRC failure **212** and column CRC **226**; Ok—null from row CRC **216**; Damaged—null from row CRC **218**; and Damaged$_{PFN}$—null from row CRC failure **212**. There is no second status because of column CRC failure **221**

Referring to FIG. **9B3** authentication then starts on each damaged or damaged$_{PFN}$ pixel with attempts to recover the original value of that element. Additional processing efforts are not made to distinguish between true negatives and false negatives due to the fact that the same damaged element recovery (DER) procedures are used on each.

To recover the value of a damaged primary image pixel the corresponding backup image pixel must first be located and validated. Validation of the corresponding backup image pixel can occur under either of the two scenarios. In the first scenario, the backup image ROW CRC for the corresponding backup image pixel is undamaged and the computed backup image ROW CRC matches the original backup image ROW CRC. In the second scenario, the backup image COLUMN CRC for the corresponding backup image pixel is undamaged and the computed backup image COLUMN CRC matches the original backup image COLUMN CRC.

Stepping **227** through each damaged or damaged$_{PFN}$ pixel in the primary image is done to locate **228** the corresponding pixel in the backup image. The backup-image will require decompression first. If the corresponding backup image pixel cannot **229** be located, it cannot be authenticated and it is not possible to recover the value of the primary image pixel **230**. Once the corresponding backup image pixel is **231** located, a self test **232** is performed on the backup image ROW CRC.

If the backup image ROW CRC self test fails **233** the backup image ROW CRC is damaged and is unusable for authentication. The backup image COLUMN CRC for the corresponding backup image pixel is then used for authentication and a self test **235** of the backup image COLUMN CRC is performed.

If the backup image COLUMN CRC for the corresponding backup image pixel fails **236** the self test, the corresponding backup image pixel cannot be authenticated and it is not possible to recover the value of the primary image pixel **230**. If the backup image COLUMN CRC for the corresponding backup image pixel passes **239** the self test then a new backup image COLUMN CRC is computed **240**.

If the new backup image COLUMN CRC matches **241** the original backup image COLUMN CRC **238** the corresponding backup image pixel is authentic and can be used to recover the value of the damaged or damaged$_{PFN}$ primary image pixel. If the new backup image COLUMN CRC does not match **243** the original backup image COLUMN CRC, the corresponding backup image pixel cannot be authenticated and it is not possible to recover the value of the primary image pixel **230**.

If the backup image ROW CRC self test succeeds **234** a new backup image ROW CRC is computed **251**. If the new backup image ROW CRC matches **237** the original backup image ROW CRC then **238** the corresponding backup image pixel is authentic and can be used to recover the value of the damaged or damaged$_{PFN}$ primary image pixel. If the new backup image ROW CRC does not **242** match the original backup image ROW CRC, one or more of the backup image pixels in that row is damaged and the backup image column must be tested for authentication.

A self test **235** of the backup image COLUMN CRC is performed. If the backup image COLUMN CRC for the corresponding backup image pixel fails **236** the self test, the corresponding backup image pixel cannot be authenticated and it is not possible to recover the value of the primary image pixel **230**. If the backup image COLUMN CRC for the corresponding backup image pixel passes **239** the self test then a new backup image COLUMN CRC is computed **240**.

If the new backup image COLUMN CRC matches **241** the original backup image COLUMN CRC **238** the corresponding backup image pixel is authentic and can be used to recover the value of the damaged or damaged$_{PFN}$ primary image pixel.

If the new backup image COLUMN CRC does not match **243** the original backup image COLUMN CRC then the corresponding backup image pixel cannot be authenticated and it is not possible to recover the value of the primary image pixel **230**.

Each pixel may then be marked in one of eight ways: Ok—ok, from row CRC **216** and column CRC **226**; Damaged—ok, from row CRC **218** and column CRC **226**; Damaged$_{PFN}$—ok, from row CRC failure **212** and column CRC **226**; Ok—null, from row CRC **216**; Damaged—null—recovered, from row CRC **218** (The original value of the pixel was recovered **238**); Damaged—null—not recovered, from row CRC **218** (the original value of the pixel was not **230** recovered); Damaged$_{PFN}$—null—recovered, from row CRC failure **212** (the original value of the pixel was recovered **238**); and Damaged$_{PFN}$—null—not recovered, from row CRC failure **212** (the original value of the pixel was not **230** recovered). Damaged—null and Damaged$_{PFN}$—null are replaced with the results of the recovery efforts

Referring to FIG. **9B4** once the authentication and recovery operations are completed the user is presented **244** with a list of eleven presented display options **245**. Option A display only the original image without any modification Option B display the original image with damaged and damaged$_{PFN}$ pixels forced to white. Option C display the original image with damaged and damaged$_{PFN}$ pixels forced to black. Option D display the original image with damaged and damaged$_{PFN}$ pixels replaced with recovered pixels. Unrecovered damaged and damaged$_{PFN}$ pixels are forced to white. Option E display the original image with damaged and dam aged$_{PFN}$ pixels replaced with recovered pixels. Unrecovered damaged and damaged$_{PFN}$ pixels are forced to black.

Rapidly displaying two alternating images is known as "rocking." Option F rocks between A and B. Option G rocks between A and C. Option H rocks between A and D. Option I rocks between A and E.

Option J displays the Statistical Report containing the various elements. This option displays the total number of pixels in the image J1. It also displays the total number of pixels marked ok—ok, Damaged—ok, Damaged$_{PFN}$—ok and ok—null, expressed as a number, and as a relative percent of the total number of pixels (J2/J1)*100 known as the "Undamaged Percentage" J2. Ok—ok pixels are those that passed both row **216** and column **226** CRC test. Ok—null pixels are those that passed the row **216** CRC test, but the column CRC was damaged **221** and provided no additional information. Damaged—ok pixels are those that were not actually damaged. The pixels were marked damaged because the new row CRC did not match **217** the original row CRC and the whole row was marked **218** damaged. These pixels passed **225** the column CRC test. Damaged$_{PFN}$—ok pixels were those that were not actually damaged. The pixels were marked damaged$_{PFN}$ because of row CRC failure **211** caused the entire row to be marked **212** Damaged$_{PFN}$. The pixels passed **225** the column CRC test.

Option J also displays the total number of damaged—null—recovered pixels as a number, and as a relative percent of the total number of pixels (J3/J1)*100 known as the "Damaged and Recovered Percentage" J3. The total number of damaged —null—not recovered pixels are also displayed as a number and as a relative percent of the total number of pixels (J4/J1)*100 known as the "Damaged and Not Recovered Pecentage" J4.

Option J displays the total number of damaged$_{PFN}$—null—recovered pixels as a number and as a relative percent of the total number of pixels (J5/J1)*100 known as the "Damaged$_{PFN}$ and Recovered Pecentage" J5. It also displays the total number of damaged$_{PFN}$—null—not recovered pixels as a number and as a relative percent of the total number of pixels (J6/J1)*100 known as the "Damaged$_{PFN}$ and Not Recovered Pecentage" J6. The sum of J2 J3 J4 J5 and J6 should equal J1, and the sum of the relative percents of J2 J3 J4 J5 and J6 should equal 100%.

The final option that may be selected is Option K to end display options. The user may continue to select **246** alternate display options until they elect to end display options **247**. At that point ELA/DER operations are concluded.

The following is information on True Negatives, False Negatives and False. Positives using row/column authentication (RCA) given that an authenticator program has been acquired from a trusted source and is free from alteration.

If a pixel is damaged (altered from its original state) and this damage is detected by the RCA operations then the pixel is a true-negative, part of an image properly determined not to be authentic. Using RCA it is possible to generate a false negative, that is where a pixel is in fact authentic, but is being marked as damaged.

There are eight possible cases of pixel authenticity/damage, row CRC authenticity/damage, and column CRC authenticity/damage.

Case	A	B	C	D	E	F	G	H
Pixel Damaged	N	Y	N	N	Y	Y	N	Y
Row CRC Damaged	N	N	Y	N	Y	N	Y	Y
Col CRC Damaged	N	N	N	Y	N	Y	Y	Y

Y = damaged
N = not damaged or ok

The number of possibilities can be expressed as

$$\frac{\text{(The number of elements)!}}{\text{(Number of identical elements)!}}$$

There are three elements in all cases. Case A is the case in which none of the three items are damaged. There is the single case with zero Y and three N. (3!/3!=1) Cases B through D are the cases in which a single item of the three are damaged. There are three cases with one Y and two N. (3!/2!=3.) Cases E through G are the cases in which two of the three items are damaged. There are three cases with two Y and one N.(3!2!=3.) Case H is the case in which three of the three items are damaged.; There is one case with three Y and zero N (3!/3!=1.)

Only in case G where both the row CRC and column CRC are damaged, and the pixel is not damaged, would a false negative be generated. Failure **189** of the row CRC self test would cause all the pixels in the row to be marked damaged$_{PFN}$ **190**. The column. CRC would also fail **198** the column CRC self test and the pixel would remain marked as damaged$_{PFN}$. In case H, both the row CRC and column CRC are damaged and would appear to mimic case. G, except that this is not a false negative because the pixel is also damaged.

Using the same table it can be shown that a false positive (a damaged pixel being improperly authenticated as undamaged) is not a possible condition. Cases B, E, F, and H have damaged pixels. In case B, the row CRC is undamaged and the newly computed **192** row CRC would not **193** match the original row CRC. Thus all pixels in the row would be marked **190** as damaged. In case B the column CRC is also undamaged. The computed new column CRC **201** would not **202** match the original CRC and the pixels in the column marked as damaged would remain marked as damaged. Only if the new column CRC matches the original column CRC **203** would all the pixels in the column, including the damaged one, be marked **204** as ok.

In case E, the row CRC is damaged and it would fail **189** the row CRC self test **188** causing all pixels in the row to be marked **208** as damaged$_{PFN}$. The column CRC is undamaged and would pass **200** the column CRC self test. The new column CRC would not **202** match the original CRC and the pixels in the column marked as damaged$_{PFN}$ would remain marked as damaged due to the fact that when a row CRC is damaged, the row of pixels is marked as "damaged potential false negative" or damaged$_{PFN}$. Only if the new column CRC matches the original column CRC **203** would all the pixels in the column, including the damaged one, be marked **204** as ok.

In case F, the row CRC is undamaged and would pass **191** the row CRC self test **188**. The newly computed row CRC **192** would not match **193** the original row CRC causing all of the pixels in the row to be marked **190** damaged. In case F, the column CRC is damaged and it would not **198** pass the CRC self test and the pixels in the column marked as damaged would remain marked as damaged.

In case H, the row CRC is damaged and would fail **189** the row CRC self test **188** causing all pixels in the row to be marked **208** as damaged$_{PFN}$. In case H, the column CRC is damaged and would not **198** pass the CRC self test. The pixels in the column marked as damaged$_{PFN}$ would remain marked as damaged$_{PFN}$ due to the fact that when a row CRC is damaged, the row of pixels is marked as "damaged potential false negative" or damaged$_{PFN}$.

Under RCA, false positives, a damaged, pixel being improperly authenticated as undamaged, cannot occur if the authenticator program has been acquired from a trusted source and is free from alteration

The following is information on True Negatives, False Negatives and False Positives using element level authentication (ELA) with damaged element recovery (DER). If a pixel is damaged (altered from its original state) and the damage is detected by the ELA operations then the pixel is a true-negative, part of an image properly determined not to be authentic. Using ELA it is possible to generate a false-negative, that is where a pixel is in fact authentic, but is being marked as damaged.

There are sixty-four (64) possible cases of primary image pixel authenticity/damage, backup image pixel authenticity/damage, primary row CRC authenticity/damage, backup row CRC authenticity/damage, primary column authenticity/damage, and backup column CRC authenticity/damage.

In table form these cases are

Y=damaged N=not damaged or ok

Group 1 Primary Image pixel is authentic and Backup Image pixel is authentic																
Case	A1	B1	C1	D1	E1	F1	G1	H1	I1	J1	K1	L1	M1	N1	O1	P1
Primary Image Pixel	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Backup Image Pixel	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Primary-Row CRC	N	Y	N	N	N	Y	Y	Y	N	N	N	Y	Y	Y	N	Y
Backup-Row CRC	N	N	Y	N	N	Y	N	N	Y	Y	N	Y	Y	N	Y	Y
Primary-Column CRC	N	N	N	Y	N	N	Y	N	Y	N	Y	Y	N	Y	Y	Y
Backup-Column CRC	N	N	N	N	Y	N	N	Y	N	Y	Y	N	Y	Y	Y	Y

-continued

Group 2 Primary Image pixel is damaged and Backup Image pixel is authentic

Case	A2	B2	C2	D2	E2	F2	G2	H2	I2	J2	K2	L2	M2	N2	O2	P2
Primary Image Pixel	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Backup Image Pixel	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Primary-Row CRC	N	Y	N	N	N	Y	Y	Y	N	N	N	Y	Y	Y	N	Y
Backup-Row CRC	N	N	Y	N	N	Y	N	N	Y	Y	N	Y	Y	N	Y	Y
Primary-Column CRC	N	N	N	Y	N	N	Y	N	Y	N	Y	Y	N	Y	Y	Y
Backup-Column CRC	N	N	N	N	Y	N	N	Y	N	Y	Y	N	Y	Y	Y	Y

Group 3 Primary Image pixel is authentic and Backup Image pixel is damaged

Case	A3	B3	C3	D3	E3	F3	G3	H3	I3	J3	K3	L3	M3	N3	O3	P3
Primary Image Pixel	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Backup Image Pixel	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Primary-Row CRC	N	Y	N	N	N	Y	Y	Y	N	N	N	Y	Y	Y	N	Y
Backup-Row CRC	N	N	Y	N	N	Y	N	N	Y	Y	N	Y	Y	N	Y	Y
Primary-Column CRC	N	N	N	Y	N	N	Y	N	Y	N	Y	Y	N	Y	Y	Y
Backup-Column CRC	N	N	N	N	Y	N	N	Y	N	Y	Y	N	Y	Y	Y	Y

Group 4 Primary Image pixel is damaged and Backup Image pixel is damaged

Case	A4	B4	C4	D4	E4	F4	G4	H4	I4	J4	K4	L4	M4	N4	O4	P4
Primary Image Pixel	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Backup Image Pixel	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Primary-Row CRC	N	Y	N	N	N	Y	Y	Y	N	N	N	Y	Y	Y	N	Y
Backup-Row CRC	N	N	Y	N	N	Y	N	N	Y	Y	N	Y	Y	N	Y	Y
Primary-Column CRC	N	N	N	Y	N	N	Y	N	Y	N	Y	Y	N	Y	Y	Y
Backup-Column CRC	N	N	N	N	Y	N	N	Y	N	Y	Y	N	Y	Y	Y	Y

In order to be a false negative: (1) the primary image pixel must be, in fact, undamaged (N); (2) initial operations must improperly indicate that the primary image pixel is damaged; and (3) all subsequent operations must fail to correct that improper indication.

The factor that in a false negative the primary image pixel must be, in fact, undamaged (N) limits the results to Group 1 and Group 3. The primary row CRC must be damaged (Y) to initially mark a row of PI pixels as damaged$_{PFN}$. If the ROW CRC is undamaged and the row of pixels is undamaged, then pixel will be marked ok. This is not a negative, false or otherwise and limits the results to cases B, F, G, H, L, M, N and P in Group 1 and Group 3.

The primary column CRC must be damaged (Y) to preclude the correction of a pixel marked damaged by a damaged row CRC. In cases B, F, H, and M, the primary column CRC is undamaged (N) which would correct the improper identification of the pixel as damaged$_{PFN}$ limiting the results to cases G, L, N and P in Group 1 and Group 3.

The backup row CRC must be damaged (Y) to preclude correction. In cases G and N, the backup row CRC is undamaged (N) and would correct the improper identification of the pixel as damaged limiting the results to case L and P in Group 1 and Group 3.

The backup column CRC must be damaged (Y) to preclude correction. In case L, the backup column CRC is not damaged (N) and would correct the improper identification of the pixel as damaged$_{PFN}$. In case P1 the backup image pixel is also authentic, but because of the damage to all of the error detection structures (primary crow CRC, primary column CRC, backup row CRC and backup column CRC) it cannot be validated as authentic. Only in cases P1 and P3 could an authentic pixel be marked damaged without the possibility of correction.

Using the same tables it can be shown that a false positive (a damaged pixel being improperly authenticated as undamaged) is not a possible condition. Group 2 and, Group 4 both contain damaged primary image pixels. If the primary row CRC is damaged, all pixels in the, row are marked damaged. If the primary row CRC is undamaged, the new row CRC will not match the provided row CRC and all pixels in the row will be marked damaged. For the purposes of isolating a case of false positive, it does not matter if the primary row CRC is damaged (Y) or not (N). The pixel will

ADOBE – Exhibit 1002, page 351

JAFFE-ADOBE000385

be marked as damaged or damaged$_{PFN}$. Again, the primary image ROW CRC alone guarantees that a damaged pixel will be marked damaged or, damaged$_{PFN}$.

To be a false positive all detective and corrective mechanisms must fail in a mode to change the primary row CRC determination that the pixel is damaged or damnmaged$_{PFN}$. If the primary column CRC is damaged **221** it will not change the determination that a pixel is damaged. If the primary column CRC is undamaged **222** the new PI COLUMN CRC will not match the original PI COLUMN CRC. Thus, it will not change the determination that a damaged pixel is damaged. For the purposes of isolating a case of false positive it does not matter if the primary column CRC is damaged (Y) or not (N). The damage pixel will remain marked as damaged.

Backup row and column CRCs are used for damaged element recovery, not element level authentication. Thus, for the purposes of isolating a case of false positive it does not matter if the backup row CRC is damaged (Y) or not (N), and it does not matter if the backup column CRC is damaged (Y) or not (N). The damaged pixel will remain marked as damaged.

This eliminates all cases in Group 2 and Group 4 as possible sources of a false positive condition. As no other cases remain for consideration, false positives are not possible if the authentication program is free from unauthorized alteration.

Using the same tables we can determine if a damaged pixel can or cannot be recovered from the damaged element recovery structures. To be considered for recovery a primary image pixel must be either, in fact damaged or a false-negative (a pixel marked damaged that is, in fact, undamaged). This limits consideration to damaged pixels in Groups 2 and 4 and cases P1 and P3 for the two possible false-negative situations.

The backup image pixel must be, in fact, undamaged. All Group 4 cases where the BI pixel is damaged are not recoverable due to the fact that all false positives are not possible. The backup image control structures must authenticate it the BI pixel as undamaged. The backup row CRC can be damaged which would lead to the backup image pixel being improperly considered damaged. If the backup column CRC were undamaged, it would correct the improper designation of the backup image pixel as damaged.

An undamaged backup row CRC would indicate that the backup image pixel is undamaged. A damaged backup column CRC would not change the determination of the backup row CRC that the backup image pixel is undamaged. Thus, as long as either the backup image row CRC or backup image column CRC are undamaged, an undamaged backup image pixel can be authenticated and used to recover the damaged primary image pixel. Only in cases J2 M2, O2 and P2 are both the backup image CRC structures damaged and unable to authenticate the undamaged backup image as undamaged.

In the false positive cases of P1 and P3 both of the backup CRC structures are damaged and unable to authenticate the undamaged backup image as undamaged. Therefore, in all 16 cases of Group 4 cases J2 M2, O2 and P2,a damaged primary image pixel cannot be recovered. If P1 or P3 generates a false negative, the improperly identified damaged primary image pixel cannot be recovered.

The following is information on the role of the random string in increasing the strength of the digital signature. A series of examples and explanations shows how the use of one time and random elements increase the resistance of a digital signature to successful fraudulent impersonation.

Starting with a blank image and a constant signature algorithm, any true image could be altered to blank and the signature from a truly blank image could be added. The resulting altered image would be improperly validated as authentic with little effort. Clearly this is a weaker situation and an undesirable outcome as the same image generates the same signature.

In the adaptive signature, a signature is generated from the contents of the image. In the case of a blank image, the same signature would be generated. An image could be manipulated to blank and the signature duplicated from a properly signed blank image. This would allow the improper validation as authentic in a manner similar to the preceding with the same undesirable outcome.

An example of an adaptive signature is one that contains a one-time element. The addition of a one-time element allows for differing signatures even if the image itself is blank. One-time elements are never repeated such as date-time or image sequence number. Some convolution or manipulation of these one-time elements is desirable to preclude their easy forgery. This is a stronger solution as the same image generates differing signatures.

An adaptive signature may also be a signature that contains one-time elements and random elements. A "random string" is a sequence of characters generated from many variables including selected values from a previous image. The algorithm to create the random string is a trade secret and may differ from device to device even among the same production run of otherwise identical devices. The algorithm used may also vary from use to use of the same device. Two blank images captured a second apart with the same device can generate two widely different signatures. Two blank images captured at the exact same moment by two different devices can generate two widely different signatures. This creates a stronger solution than the adaptive signature containing only a one-time element.

Another variation is an adaptive signature with a one-time element and a one-time random element. The user has control over how often a new random string is created. If the random string were created anew after each image was captured, then pattern recognition of the resulting signature from the image is not possible as random elements are, by definition, not patterned. Unless the signature generation protocol and the random string generation algorithm were known or reverse engineered, the ability to sign a properly constituted Signa2 image resides solely inside the Signa2 devices. By varying the random string generation protocol between devices, varying between protocols between use to use of the same device, and regenerating the random string frequently, analysis of the results to determine the process (a form of reverse engineering) is an almost fruitless exercise.

While the invention has been illustrated and described in detail in the drawings and foregoing description, the same is considered as illustrative and not restrictive in character, it being understood that all changes and modification that come within the spirit of the invention are desired to be protected.

What is claimed is

1. A method for authenticating a data stream stored in a data file in memory, said method comprising the steps of:

storing a data stream in a data file in a memory;

utilizing a sensor, which is tightly coupled to said memory, to generate at least one internal and unique parameter;

monitoring the integrity of the tight coupling between said memory and said sensor when said at least one internal and unique parameter is generated, and, if said integrity

is compromised, then also providing an indication of said compromised integrity;

utilizing a signature protocol to generate a first signature based on said data stream and said at least one parameter, said first signature being generated without altering said data stream and being appended to said data file in said memory;

utilizing said signature protocol to generate a second signature based on said image;

comparing said first signature to said second signature,

if said first and second signatures are not the same, then generating an error signal that is displayed to a user to indicate that said stored data stream is not authentic, and

if said first and second signatures are the same, then generating an ok signal that is displayed to a user to indicate that said stored data stream is authentic.

2. The method of claim 1, wherein said memory form a part of a digital camera.

3. The method of claim 1, wherein said at least one parameter comprises a random number.

4. The method of claim 1, further comprising the step of appending at least one additional parameter to said data file in said memory, said at least one additional parameter being generally representative of a condition under which said data stream was generated.

5. The method of claim 4, wherein said at least one additional parameter is selected from a group consisting of: GPS coordinates, zoom settings, AutoFocus status, focus quality sampling, roll, pitch and yaw values, compass headings, flash status, CamID, Seq, and a Security Value.

6. The method of claim 1 wherein said data stream is a digit sample of an environment.

* * * * *

PATENT APPLICATION FEE DETERMINATION RECORD
Effective December 29, 1999

Application or Docket Number

CLAIMS AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA
BASIC FEE		
TOTAL CLAIMS	8 minus 20=	* —
INDEPENDENT CLAIMS	2 minus 3 =	* —
MULTIPLE DEPENDENT CLAIM PRESENT		

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE ☐	RATE	FEE	OR	OTHER THAN SMALL ENTITY	RATE	FEE
		345.00	OR			690.00
	X$ 9=		OR		X$18=	
	X39=		OR		X78=	
	+130=		OR		+260=	
	TOTAL		OR		TOTAL	

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 6	Minus	** 8	= —
Independent	* 1	Minus	*** 2	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

SMALL ENTITY	RATE	ADDI-TIONAL FEE	OR	OTHER THAN SMALL ENTITY	RATE	ADDI-TIONAL FEE
	X$ 9=		OR		X$18=	
	X39=		OR		X78=	
	+130=		OR		+260=	
	TOTAL ADDIT. FEE		OR		TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

RATE	ADDI-TIONAL FEE	OR	RATE	ADDI-TIONAL FEE
X$ 9=		OR	X$18=	
X39=		OR	X78=	
+130=		OR	+260=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

RATE	ADDI-TIONAL FEE	OR	RATE	ADDI-TIONAL FEE
X$ 9=		OR	X$18=	
X39=		OR	X78=	
+130=		OR	+260=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
***If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

ISSUE SLIP STAPLE AREA (for additional cross references)

POSITION	INITIALS	ID NO.	DATE
FEE DETERMINATION	D.R.	2200	8-4-00
O.I.P.E. CLASSIFIER			
FORMALITY REVIEW		64665	8-11-00
RESPONSE FORMALITY REVIEW			

INDEX OF CLAIMS

✓ ..... Rejected
= ..... Allowed
— (Through numeral)... Canceled
÷ ..... Restricted
N ..... Non-elected
I ..... Interference
A ..... Appeal
O ..... Objected

Claim Final	Claim Original	Date
	1	8/2/00 11/16/00
	2	✓ —
	3	
	4	
	5	
	6	
	7	
	8	✓ —
	9	✓ =
2	10	✓ =
3	11	=
4	12	=
5	13	=
6	14	✓ =
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim Final	Claim Original	Date
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim Final	Claim Original	Date
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

If more than 150 claims or 10 actions
staple additional sheet here

(LEFT INSIDE)

SEARCHED

Class	Sub.	Date	Exmr.
713	176	8/12/03	HS
	168		
380	258		
	229		
	200		
348	207.99	4/6/04	HS
382	276		
	312-313		
713	161, 168		
	176, 200		
380	258		
	54, 46		
	200		
all updated as of		4/6/04	HS

INTERFERENCE SEARCHED

Class	Sub.	Date	Exmr.
713	168, 176	4/6/04	HS
	200		
382	312-313		
	276		
348	207.99		
380	258, 54,		
	46; 200		

SEARCH NOTES
(INCLUDING SEARCH STRATEGY)

	Date	Exmr.
EAST	8/12/03	HS
NPL search		
EPO, DERWENT		
Inventor name search		
EAST search	2/12/04	HS
EAST search foreign patent database search DIALOG search	4/6/04	HS

(RIGHT OUTSIDE)

PATENT APPLICATION

09626044

jc862 U.S. PTO
09/626044
07/27/00

AUG 10 00 12
INITIALS

CONTENTS

		Date Received (Incl. C. of M.) or Date Mailed			Date Received (Incl. C. of M.) or Date Mailed
1	Application papers.		42.		
2			43.		
3	Ref (3mos)	7/3/03	44.		
	Advance	1.8			
4	Final Rej (3)	2/24/04	45.		
5	RCE	3-1-04	46.		
6.	Pre-B	3-1-04	47.		
7.	Notice of allow	4/20/04	48.		
8.			49.		
9.			50.		
10.			51.		
11.			52.		
12.			53.		
13.			54.		
14.			55.		
15.			56.		
16.			57.		
17.			58.		
18.			59.		
19.			60.		
20.			61.		
21.			62.		
22.			63.		
23.			64.		
24.			65.		
25.			66.		
26.			67.		
27.			68.		
28.			69.		
29.			70.		
30.			71.		
31.			72.		
32.			73.		
33.			74.		
34.			75.		
35.			76.		
36.			77.		
37.			78.		
38.			79.		
39.			80.		
40.			81.		
41.			82.		

(LEFT OUTSIDE)