US 20070052730A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2007/0052730 A1**

Patterson et al. (43) **Pub. Date: Mar. 8, 2007**

(54) **IMAGE MANAGEMENT SYSTEM AND METHODS USING DIGITAL WATERMARKS**

(76) Inventors: **Phillip R. Patterson**, Sherwood, OR (US); **Lorie Clements**, Portland, OR (US); **Neil A. Lofgren**, Portland, OR (US); **Geoffrey B. Rhoads**, West Linn, OR (US)

Correspondence Address:
DIGIMARC CORPORATION
9405 SW GEMINI DRIVE
BEAVERTON, OR 97008 (US)

(21) Appl. No.: **11/468,258**

(22) Filed: **Aug. 29, 2006**

Related U.S. Application Data

(63) Continuation of application No. 09/858,336, filed on May 15, 2001, now Pat. No. 7,098,931, and which is a continuation-in-part of application No. 09/800,093, filed on Mar. 5, 2001, now Pat. No. 7,061,510.

(60) Provisional application No. 60/284,163, filed on Apr. 16, 2001. Provisional application No. 60/284,776, filed on Apr. 18, 2001.

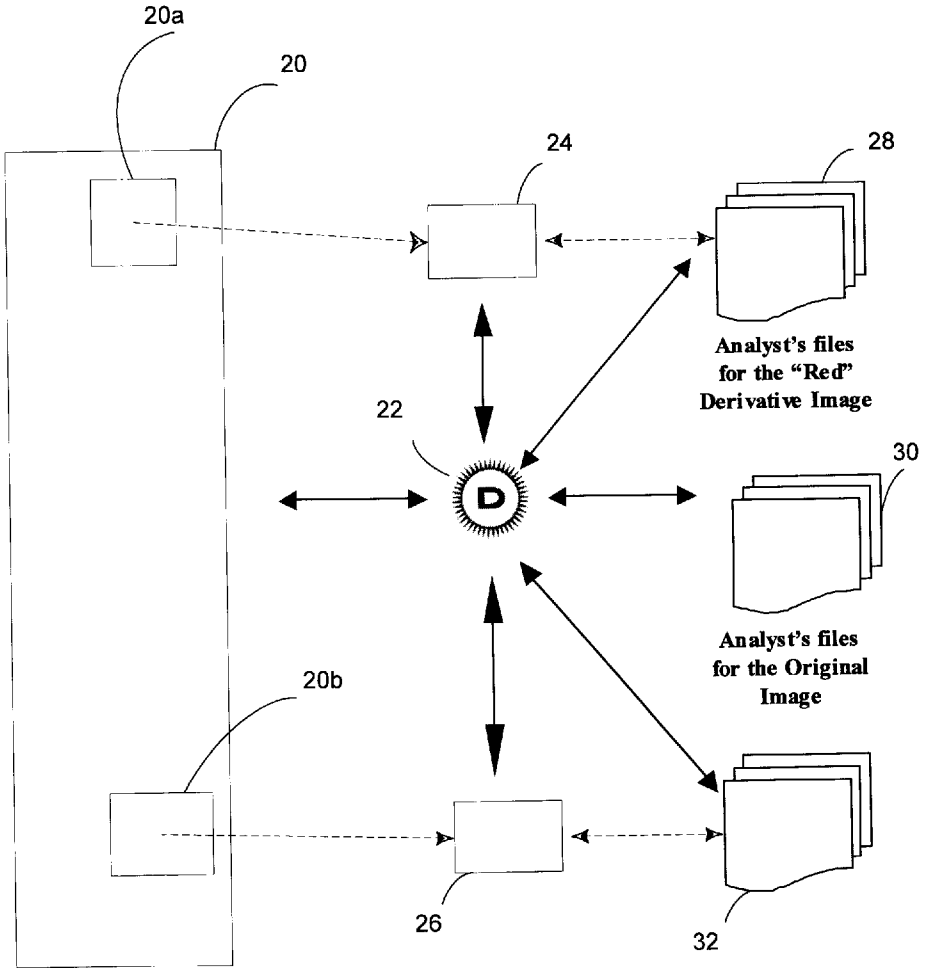
Publication Classification

(51) **Int. Cl.**
G09G 5/00 (2006.01)

(52) **U.S. Cl.** **345/634**

(57) **ABSTRACT**

Digital watermarking technology is used in an image management system. Images are uniquely identified by digital watermarking. The images are stored so as to be indexed according to unique identifiers. In one embodiment, related images are linked together by a unique watermark identifier. The unique watermark identifier is also used to manage metadata, and provide forensic tracking. Watermark identifiers can be used to carry or access security clearance information associated with an image or other media. Other embodiments are provided as well.



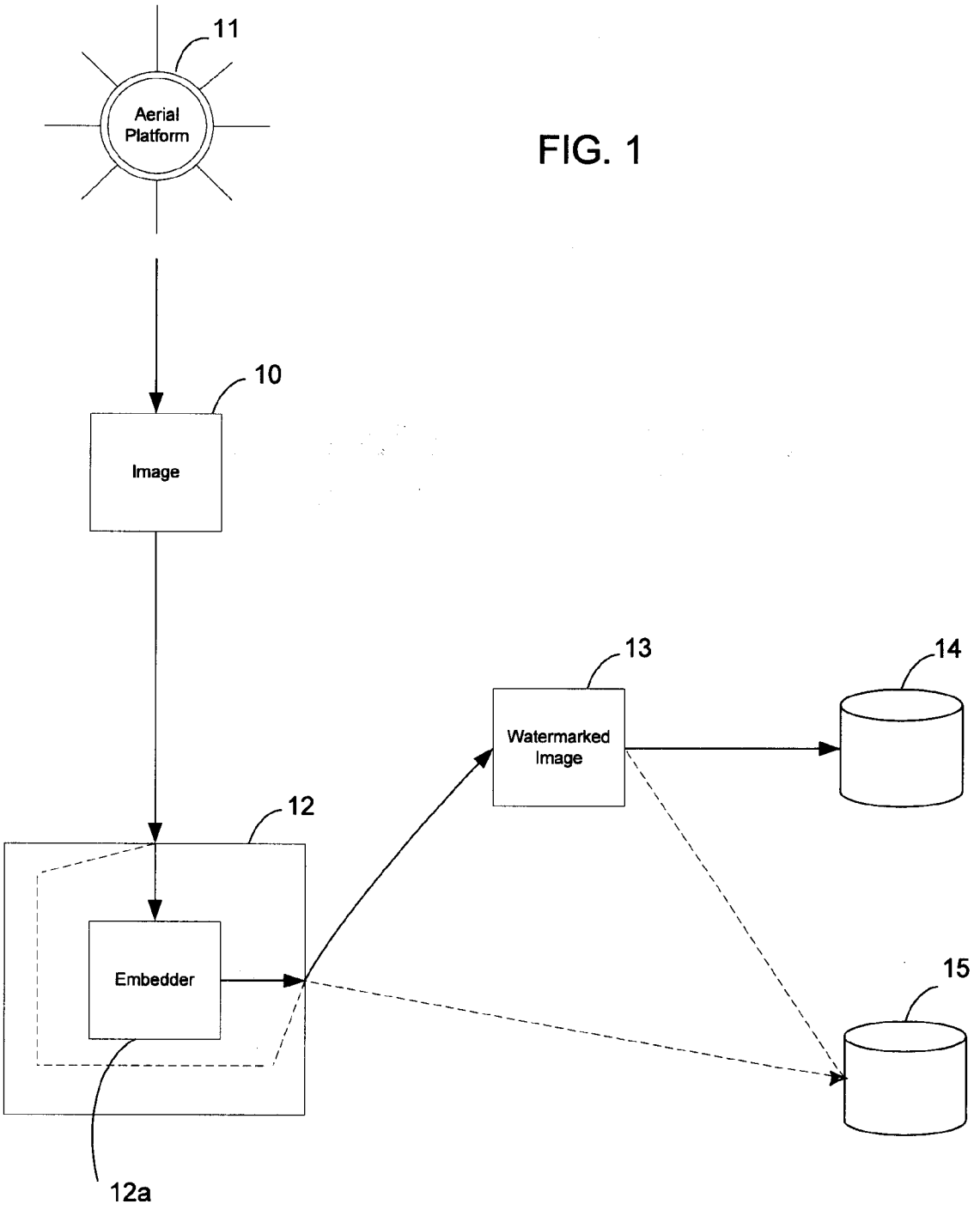

11
Aerial Platform
10
Image
13
Watermarked Image
14
12
Embedder
15
12a

FIG. 1

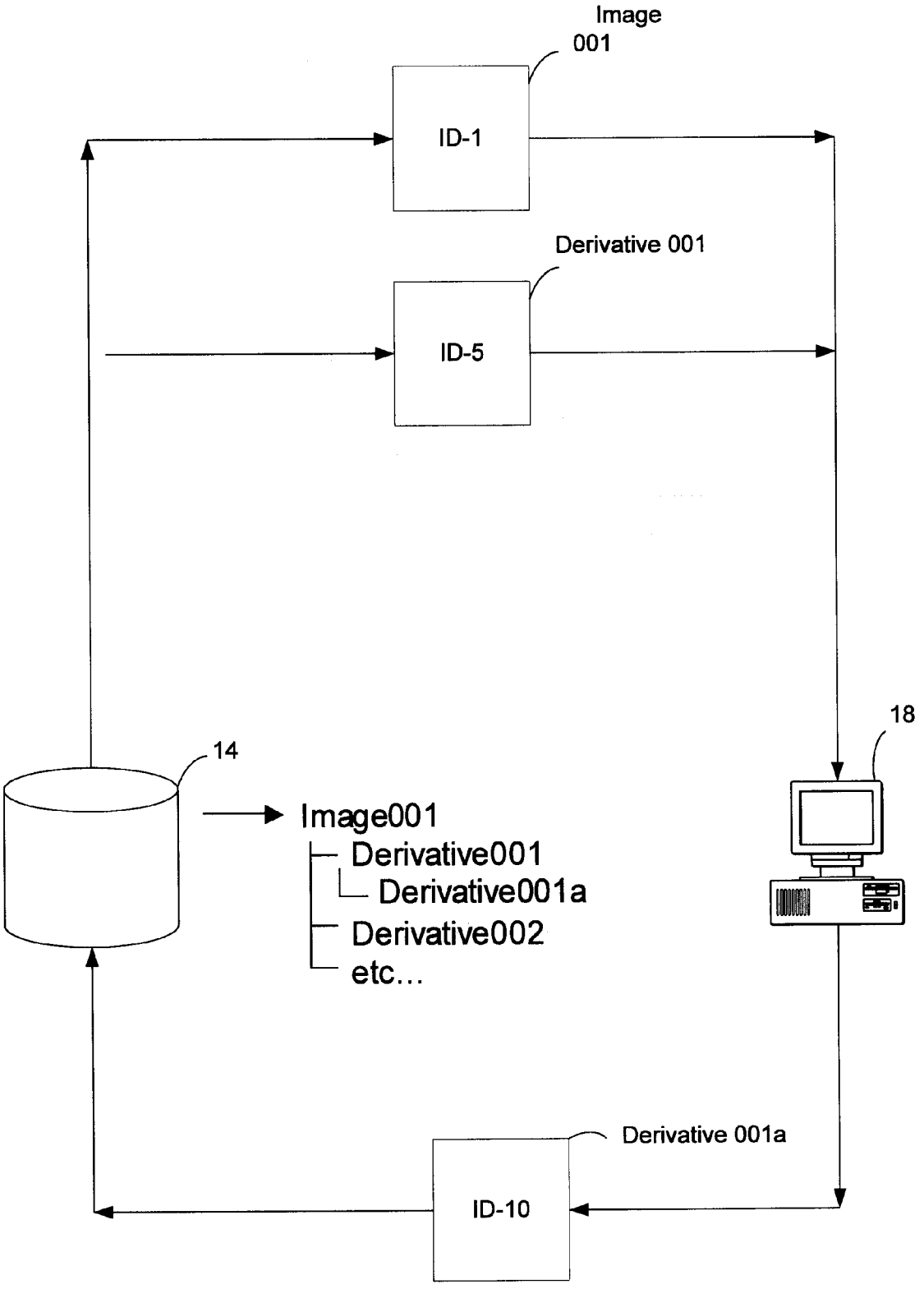


Image
001
ID-1
Derivative 001
ID-5
18
14
Image001
Derivative001
Derivative001a
Derivative002
etc...
Derivative 001a
ID-10

FIG. 2

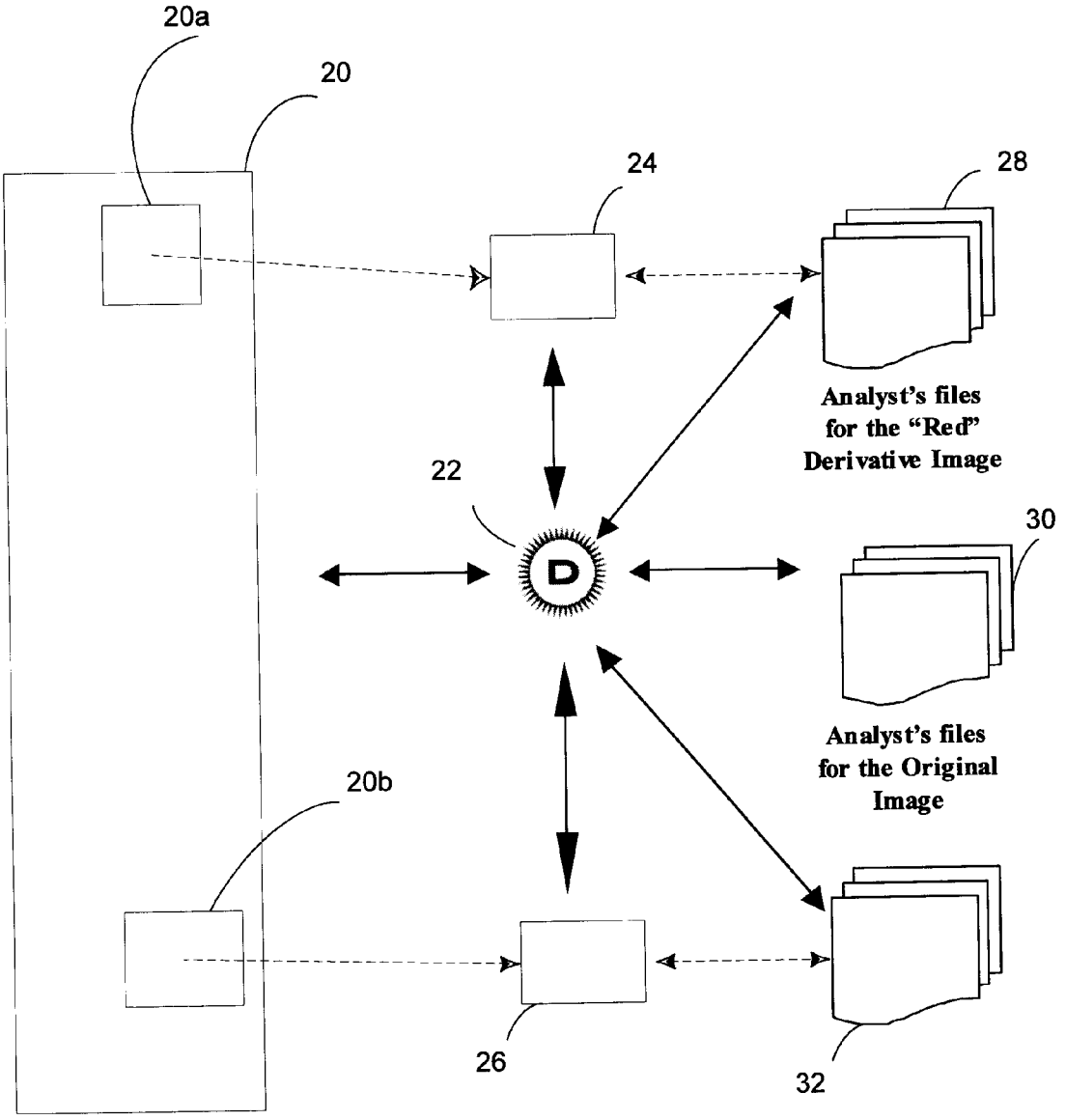

20a
20
24
28
Analyst's files for the "Red" Derivative Image
22
D
30
Analyst's files for the Original Image
20b
26
32

FIG. 3

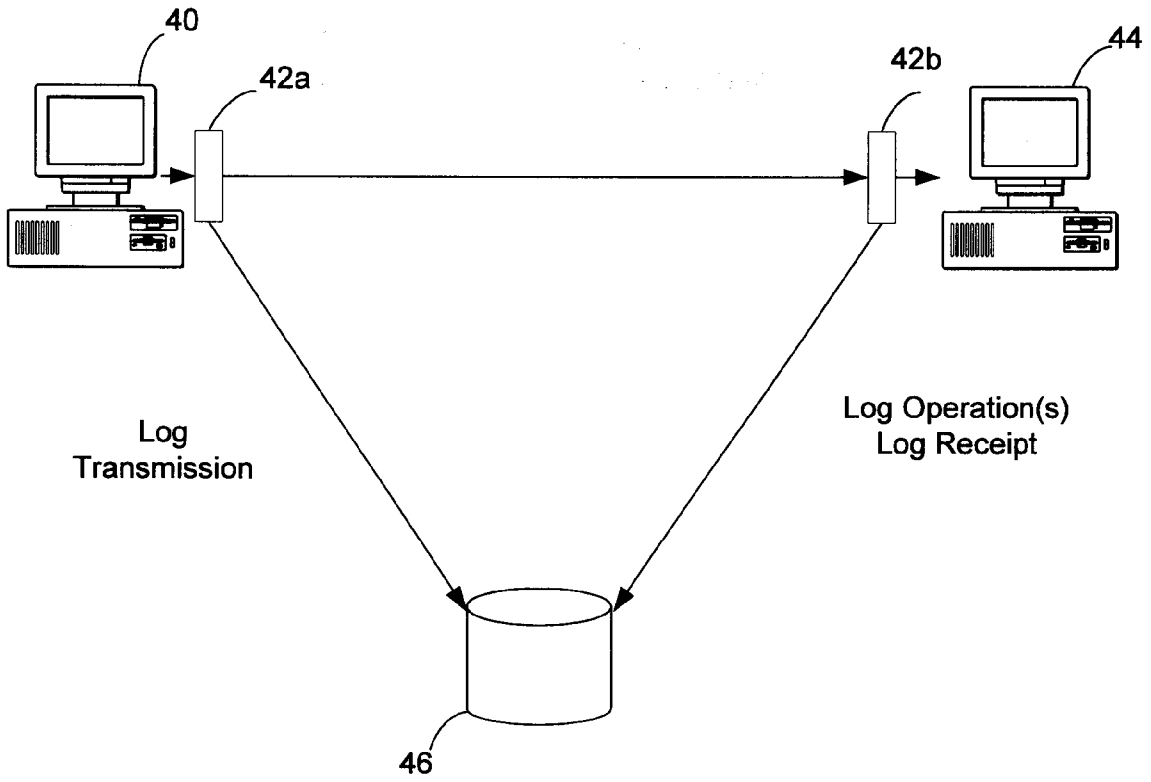

40
42a
42b
44
Log
Transmission
Log Operation(s)
Log Receipt
46

FIG. 4

FIG. 5

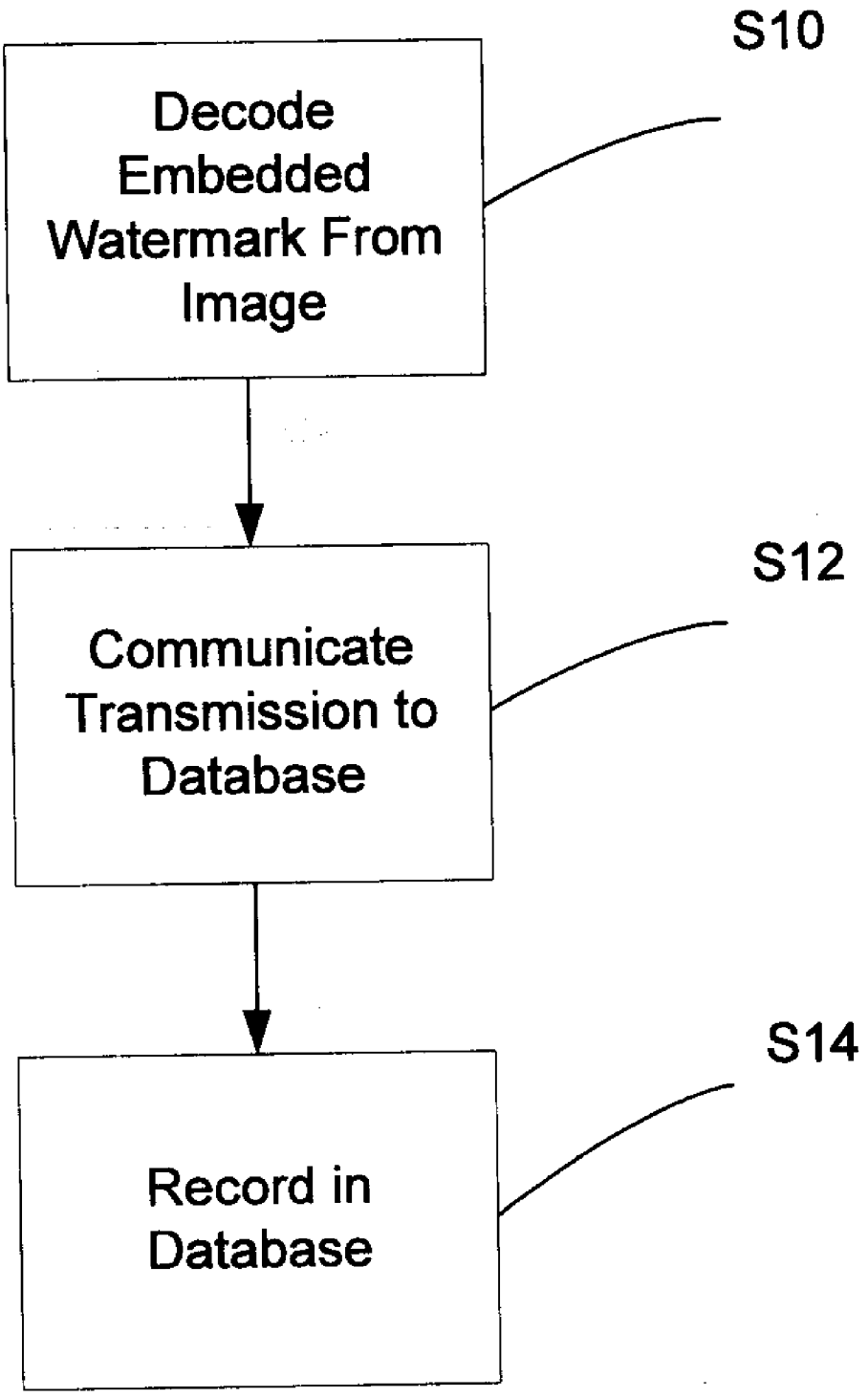

S10
Decode Embedded Watermark From Image
S12
Communicate Transmission to Database
S14
Record in Database

FIG. 6

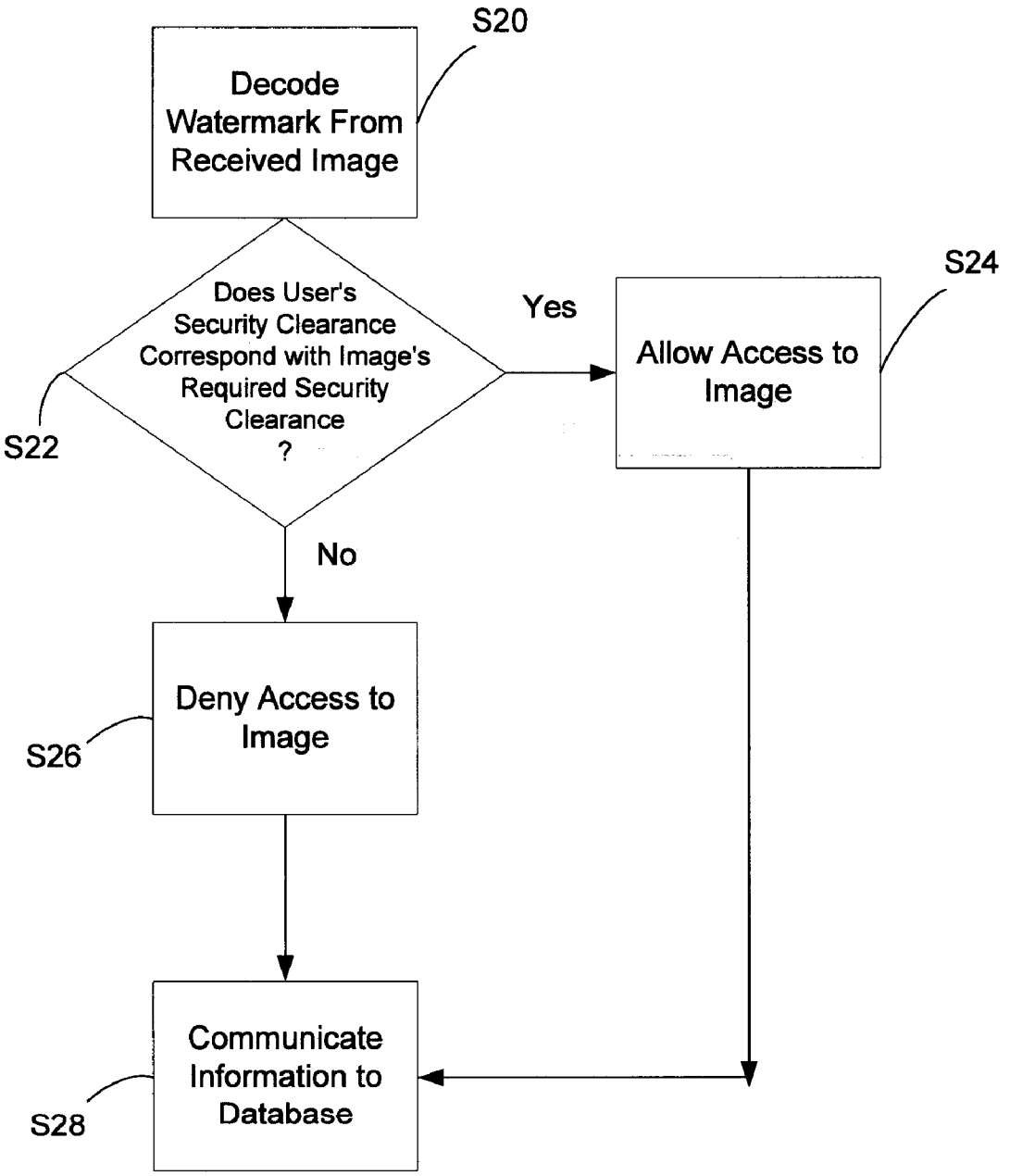

S20
Decode Watermark From Received Image
Does User's Security Clearance Correspond with Image's Required Security Clearance ?
S22
Yes
S24
Allow Access to Image
No
Deny Access to Image
S26
Communicate Information to Database
S28

IMAGE MANAGEMENT SYSTEM AND METHODS USING DIGITAL WATERMARKS

RELATED APPLICATION DATA

[0001] This application is a continuation of U.S. patent application Ser. No. 09/858,336, filed May 15, 2001 (issuing as U.S. Pat. No. 7,098,931). The U.S. Ser. No. 09/858,336 application claims the benefit of U.S. Provisional Application Nos. 60/284,163 filed Apr. 16, 2001, entitled "Watermark Systems and Methods," and 60/284,776 filed Apr. 18, 2001, entitled "Using Embedded Identifiers with Images." The 09/858,336 application is also a continuation-in-part of assignee's U.S. patent application Ser. No. 09/800,093, entitled "Geo-Referencing of Aerial Imagery Using Embedded Image Identifiers and Cross-Referenced Data Sets," filed Mar. 5, 2001 (now U.S. Pat. No. 7,061,510).

[0002] This patent application is also related to assignee's U.S. patent application Ser. No. 09/833,013, entitled "Digitally Watermarked Maps and Signs and Related Navigational Tools," filed Apr. 10, 2001 (published as US 2002-0147910 A1).

FIELD OF THE INVENTION

[0003] The present invention relates to image management and processing, and is particularly illustrated in the context of a satellite and other aerial imagery management system.

BACKGROUND AND SUMMARY OF THE INVENTION

[0004] Aerial imagery has vastly improved since the Wright brothers first took to the sky. Indeed, there have been many improvements in the photography and digital imaging fields.

[0005] While the earliest aerial imagery relied on conventional film technology, a variety of electronic sensors are now more commonly used. Some collect image data corresponding to specific visible, UV or IR frequency spectra (e.g., the MultiSpectral Scanner and Thematic Mapper used by the Landsat satellites). Others use wide band sensors. Still others use radar or laser systems (sometimes stereo) to sense topological features in 3 dimensions. Some satellites even collect ribbon imagery (e.g., a raster-like, 1-dimensional terrestrial representation, which is pieced together with other such adjacent ribbons).

[0006] The quality of the imagery has also constantly improved. Some satellite systems are now capable of acquiring image and topological data having a resolution of less than a meter. Aircraft imagery, collected from lower altitudes, provides still greater resolution.

[0007] A vast amount of aerial imagery is constantly being generated and collected. Management of the resulting large data sets is a growing problem. In today's digital world, images are routinely manipulated, even on home computers. Management of resulting image ancestry, image derivates and related metadata is increasingly difficult.

[0008] According to one aspect of the present invention, a digital watermark-based image management system helps solve these and other problems. A digital watermark is ideally employed as an enabler to access a related family of images, linked in a database (or other data structure) via digital watermark identifiers. Watermark identifiers can also be used to identify the source of an image, track images and documents, document a distribution chain, and identify unlabeled hard copy images. According to another aspect, digital watermarks help to provide security, monitoring and gatekeeper-like functions.

[0009] Digital watermarking is a form of steganography that encompasses a great variety of techniques by which plural bits of digital data are hidden in some other object without leaving human-apparent evidence of alteration.

[0010] Digital watermarking may be used to modify media content to embed a message or machine-readable code into the content. The content may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process.

[0011] Most commonly, digital watermarking is applied to media such as images, audio signals, and video signals. However, it may also be applied to other types of data, including documents (e.g., through line, word or character shifting, through texturing, graphics, or backgrounds, etc.), software, multi-dimensional graphics models, and surface textures of objects.

[0012] The assignee's U.S. Pat. No. 6,122,403, and co-pending U.S. patent application Ser. No. 09/503,881 (now U.S. Pat. No. 6,614,914), detail suitable digital watermarking techniques in which values of pixels, e.g., in a 100×100 pixel patch, can be slightly altered so as to convey a plural-bit payload, without impairing use of the pixel data for its intended purpose. The payload may be on the order of 2-256 bits, depending on the particular form of encoding (e.g., convolution, turbo, or BCH coding can be employed to provide some error-correcting capability), and the number of bits per pixel. Larger payloads can be conveyed through larger image patches. (Larger payloads can also be conveyed by encoding the information in a less robust fashion, or by making the encoding more relatively visible.). The watermark payload can convey an image identifier, and may convey other metadata as well. In some embodiments, the component image files are tagged both by digital watermark identifiers and also by conventional out-of-band techniques, such as header data, thereby affording data redundancy. Of course, there are many watermarking techniques known to those skilled in the art, and such may be suitably interchanged with the present invention.

[0013] Digital watermarking systems typically have two primary components: an embedding component that embeds the watermark in the media content, and a reading component that detects and reads the embedded watermark. The embedding component embeds a watermark pattern by altering data samples of the media content. The reading component analyzes content to detect whether a watermark pattern is present. In applications where the watermark encodes information, the reading component extracts this information from the detected watermark. Commonly assigned U.S application Ser. No. 09/503,881, filed Feb. 14, 2000, discloses various encoding and decoding techniques. U.S. Pat. No. 5,862,260 discloses still others.

[0014] Watermarking may be performed in stages, at different times. For example, a unique identifier can be water-

marked into an image relatively early in the process, and other information (such as finely geo-referenced latitude/longitude) can be watermarked later. A single watermark can be used, with different payload bits written at different times. (In watermark systems employing pseudo-random data or noise (PN), e.g., to randomize some aspect of the payload's encoding, the same PN data can be used at both times, with different payload bits encoded at the different times.).

[0015] Alternatively, different watermarks can be applied to convey different data. The watermarks can be of the same general type (e.g., PN based, but using different PN data). Or different forms of watermark can be used (e.g., one that encodes by adding an overlay signal to a representation of the image in the pixel domain, another that encodes by slightly altering DCT coefficients corresponding to the image in a spatial frequency domain, and another that encodes by slightly altering wavelet coefficients corresponding to the image. Of course, other watermarking techniques may be used as suitable replacements for those discussed above.).

[0016] In some multiple-watermarking approaches, a first watermark is applied before a satellite image is segmented into patches. A later watermark can be applied after segmentation. (The former watermark is typically designed so as to be detectable from even small excerpts of the original image.)

[0017] A watermark can be applied by an imaging instrument. In some embodiments, the image is acquired through an LCD optical shutter, or other programmable optical device, that imparts an inconspicuous patterning to the image as it is captured. (One particular optical technique for watermark encoding is detailed in U.S. Pat. No. 5,930,369.). Or the watermarking can be effected by systems in a satellite (or other aerial platform) that process the acquired data prior to transmission to a ground station. In some systems, the image data is compressed for transmission—discarding information that is not important. The compression algorithm can discard information in a manner calculated so that the remaining data is thereby encoded with a watermark.

[0018] A ground station receiving the satellite transmission can likewise apply a watermark to the image data. So can each subsequent system through which the data passes, if desired.

[0019] Preferably, such watermarking processes are secure and cannot be replicated by unauthorized individuals.

[0020] The foregoing and additional features and advantages of the present invention will be more readily apparent from the following detailed description with reference to the following figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] FIG. **1** is a functional block diagram illustrating a digital watermarking process.

[0022] FIG. **2** illustrates components of an image management system.

[0023] FIG. **3** illustrates associating related images and information with a digital watermark identifier.

[0024] FIG. **4** is a functional block diagram illustrating gatekeepers in a network.

[0025] FIGS. **5** and **6** are flow diagrams illustrating gatekeeping methods and processes according to the FIG. **4** embodiment.

DETAILED DESCRIPTION

[0026] For expository convenience, the following discussion focuses on satellite and other aerial "imagery" to illustrate the principles of the invention. The principles of the invention, however, are equally applicable to other forms of imagery, including non-aerial imagery. Accordingly, the term "image" should be used to encompass other data sets, and the term "pixel" should be construed to encompass component data from such other data sets. The term "image" should also be construed to include both digital and analog data sets.

[0027] Watermarking Images

[0028] With reference to FIG. **1**, an image (or image data) **10** is captured from an aerial platform **11**, such as an aircraft, satellite, balloon, unmanned aircraft, etc. The image **10** is communicated to a receiving or ground station **12**. (In some instances, the image signal may be relayed through various aerial and/or other ground stations before reaching ground station **12**.). Ground station **12** preferably includes a watermark embedder **12***a*, which embeds a digital watermark with the image **10**, to produce a digitally watermarked image **13**.

[0029] A digital watermark is typically embedded in a digital representation of the image **10**. Although not required, the digital watermark preferably survives transformation to various analog representations (e.g., printing) as well. The digital watermark includes a watermark identifier (ID). In the preferred embodiment, each image is digitally watermarked to include a unique watermark ID. The ID typically includes plural-bit data, e.g., in the range of 2-256 bits. In one embodiment, a digital watermark (and identifier) is redundantly embedded within an image to improve robustness. For example, an image is divided into tiles or sections, and each tile or section is embedded with the digital watermark (and ID). Alternatively, a subset of the sections are embedded. Such techniques help to ensure the robustness of a watermark, particularly when an image is to be manipulated (e.g., clipped, cut-and-pasted, resized, rotated, etc.).

[0030] Digitally watermarked image **13** is stored in a database **14**. (A watermarked image can be directly communicated to database **14**, transferred via a storage medium and/or relayed to database **14**.). Database **14** preferably manages images and/or related data. Database software, e.g., such as provided by Microsoft, Oracle, Sun Microsystems, etc., can be executed by a computer or server to help maintain database **14**. Of course, database **14** can be maintained by a ground station **12** system, or be maintained in a remotely located network. In one embodiment, database **14** communicates with a network, such as a LAN, WAN, dedicated network, private network, etc. In some embodiments, database **14** includes a plurality of databases. In this case, at least one database maintains image data, while at least a second database maintains related information (e.g., metadata, related files, comments, file history, and/or security clearance information, etc.). Here, metadata is broadly defined to include a variety of information such as creation data, geo-location information, ancestry data, security infor-

mation, access levels, copyright information, security classifications, usage rights, and/or file history, etc.

[0031] Image **13** and/or any related information is preferably stored and indexed according to watermark IDs. For example, a watermark ID provides a thread by which images and related information are grouped, stored and/or indexed. (The dashed lines in FIG. **1** represent this optional embodiment.).

[0032] Optionally, image data is communicated to a second database **15**. Database **15** can be used to maintain original image **10** and/or an original watermarked image **13**.

[0033] Image and Derivative Image Management Using Digital Watermarks

[0034] As indicated above, a problem faced by image management systems is how to efficiently manage an image's ancestry and related information. Normal image processing (e.g., scaling, cropping, rotating, clipping, resizing, cut-and-pasting image blocks, and/or marking, etc.) of an "original" image results in a "derivative" image. In conventional systems, derivative images frequently retain minimal, if any, related metadata. The metadata, such as that stored in header or footer files, is easily separable from derivative images. Separation results in a significant loss of information, particularly for a derivative image. One conventional solution is to manually record an image identifier as an image moves through an exploitation (or derivative) process. This manual recording process is labor intensive and cumbersome at best.

[0035] A better solution, as disclosed in this application, is to place a unique digital watermark ID within an image to enable database linking and indexing. Metadata contained within the database can be then associated with a specific image, or with a family of images, via the unique watermark ID. With reference to FIG. **2**, a user terminal **18** retrieves a digitally watermarked image **001** from database **14**. User terminal **18** preferably includes a processor, memory and suitable software instructions to facilitate digital watermark detection and/or embedding. The user terminal **18** will preferably include an operating system, such as Windows, Windows NT, Linux, etc., and image-handling (and editing) software. Suitable image-handling software can be obtained from Microsoft, Adobe, SRI and Erdas, among others. Preferably, both the watermark detecting software and the image-handling software are compatible with various types of image formats, such as bit-maps, JPEG files, TIF files, etc. (However, such compatibility is not required.).

[0036] Watermark detection software executing in user terminal **18** analyzes image **001**. The watermark detection software can be called by the imaging software, may operate as a plug-in, or may be even integrated with the image-handling software, operating system, or other software module. The watermark detection software extracts the unique watermark identifier (e.g., ID-**1**) embedded within image **001**. Having obtained the identifier (ID-**1**), the user terminal **18** can optionally communicate with database **14** to retrieve related information, such as metadata, files, and related images. For example, the watermark ID-**1** is used to interrogate database **14** to retrieve information regarding the geo-coordinates for the image, the time and date taken, analyst comments, and/or analyst information, etc. Preferably, the watermark ID-**1** can also be used to index any derivative images, e.g., derivative **001**. (In this case, derivative **001** is an image derived from image **001**.).

[0037] In a preferred embodiment, since each image includes a unique identifier, derivative **001** includes a watermark identifier (e.g., ID-**5**), which is unique from the corresponding original image **001** (e.g., identifier ID-**1**). Derivative **001** and image **001** are associated (e.g., linked) together in database **14**, via identifier ID-**1** (and, optionally, via ID-**5**).

[0038] In some instances, user terminal **18** will create additional derivatives. Take for instance, an example when user terminal **18** enlarges the derivative **001** image, thus creating a new derivative **001***a*. This new derivative is preferably uniquely identified with a digital watermark. A process of digitally watermarking a derivative typically involves removing the original watermark from the derivative and replacing the watermark with a new unique identifier. (In an alternative embodiment, the original watermark is altered, e.g., by changing one or more message bits, to create the new unique identifier. In another embodiment, a second watermark is added to the derivative image to complement the first (or more) watermark. In this case, the first watermark identifies the original image, and the second watermark identifies the derivative.). Preferably, upon creating derivative **001***a*, the digital watermarking software removes the derivative **001** watermark (or at least a portion of the watermark, e.g., identifier ID-**5**) from the derivative **001** image. Assignees' U.S. application Ser. No. 09/503,881 discusses some techniques for such. Artisans know others still. Derivative **001***a* is then embedded with a unique digital watermark identifier (e.g., ID-**10**).

[0039] The watermark embedding software can determine an appropriate identifier in a number of ways. In one embodiment, the embedding software queries database **14** for an appropriate, or available, identifier. In another case, embedding software (or user terminal **18**) is assigned a range of identifiers, and an identifier is chosen from the available range. In still another embodiment, the embedding software randomly or pseudo-randomly selects the identifier, or alters a portion of the original image identifier, e.g., 2-32 bits of the original watermark identifier.

[0040] An image and a watermark identifier are combined to produce a digitally watermarked image (or derivative image) preferably in the same format and density as the input image. As an optional feature, software provides an indicator to signal success or failure in the watermarking effort. For example, the software can analyze whether the watermark was embedded, and/or whether the image contains the same format and density as the original input image. Upon a failure, user terminal **18** re-embeds the digital watermark or aborts the process.

[0041] Derivative image **001***a* is stored in database **14**. Related information can also be stored in database **14**. (As discussed above, database **14** may include a plurality of databases. One such database may manage images, while another database manages related information. Preferably, however, the unique identifiers are used consistently between the plurality of databases to link related images and information.). Database **14** links derivative **001***a* with image **001**, derivative **001** and any related information (e.g., metadata, comments, files, history, security, etc.). Accordingly, image ancestry and any related information is efficiently maintained.

[0042] FIG. **3** is a diagram further illustrating linking images, derivatives and related information via a unique watermark identifier. An original image **20** is watermarked with a unique identifier **22**. A first derivative image **24** (e.g., perhaps an enlarged or cropped image corresponding with area **20***a*) and a second derivative **26** (e.g., corresponding to area **20***b*) are created. Each of the first derivative **24** and second derivative **26** are encoded with a unique watermark identifier. The derivative identifiers are associated with the unique identifier **22** in database **14**. Such linking effectively groups image families together, permitting a user to gain access to image ancestry. Similarly, related information can be linked via unique identifier **22**. Returning to FIG. **3**, related information **28** corresponding to first derivative **24** are linked to identifier **22**. Files **30** corresponding to the original image **20**, as well as files **32** for the second derivative **26**, are likewise linked. Accordingly, entire image families (and related information) are efficiently maintained by linking via the unique identifier **22**. Of course, files **28** and **30** optionally can be separately, and respectively, linked to derivatives **24** and **26**, via the derivatives' unique identifiers (e.g., as shown by the dashed lines in FIG. **3**).

[0043] Security and Rewritable Watermarks

[0044] In one embodiment, a watermark provides information related to a permission level or a security clearance level. Such information can be reflected in a unique identifier or in a payload message. Alternatively, the watermark identifier can be used to interrogate a database to retrieve related security level requirements. Such security information can be used to regulate access to images and related information. For example, only users (or user terminals) having a corresponding permission level or security clearance are allowed to access the corresponding image. Suitable software instructions can examine the permission level (or security clearance) to determine whether a user (or terminal) has the necessary clearance.

[0045] One aspect of the present invention is to employ "rewritable" watermarks. A rewritable watermark includes a watermark of which all or a portion of which may be changed. In a preferred embodiment, only a portion (e.g., a portion of the payload) of a watermark is rewritten to update permission levels, reflect derivative work, etc.

[0046] There are often situations where it is desirable to carry some form of security access indicator in an image, e.g., via a digital watermark. The security access indicator defines a level of security required to view, edit or comment with respect to an image. Access to the image is then controlled by appropriately enabled software, which extracts the indicator (or receives the indicator from a watermark decoder) and determines usage. In one embodiment, the indicator indicates defines a required level. If a user's security level is equal to or greater (e.g., as determined from a password, user terminal identifier, login, linked security clearance level, etc.) to that carried in a security access indicator, then a user is allowed access to the image or data. In another embodiment, a security code may indicate that a particular user can view the image, but cannot edit or store comments regarding such.

[0047] Consider the following example. An image "A" is defined to include an "unclassified" security classification. Image A's watermark then includes a unique identifier and additional plural-bits set to a predetermined number, e.g., all set to zero (or to a predetermined number or pattern). These additional plural-bits define the unclassified security classification. An image "B" is a derivative of image A, and has a "secret" security classification encoded in the plural-bits. Before either image A or B is opened (or requested) the security level contained within the watermark is validated against the security level of the individual requesting access, and permission is only granted to those with adequate clearance. In one embodiment, local software (e.g., executing on a user terminal) validates the security access by decoding the watermark, extracting the security bits, and comparing the security bits (or corresponding security level) with the security clearance of a user (or terminal). In another embodiment, software running on a central server monitors and validates security access. Or in another embodiment software associated with the database regulates the security access.

[0048] Application Interface

[0049] Application interface software, residing on a user terminal, helps to facilitate communication between image-handling software and database **14**. The interface can be incorporated in such image-handling software, operate as a plug-in, be integrated with the operating system, or may even be called by certain operations (e.g., data retrieval, editing, saving, etc.). Preferably, the interface generates (or works in connection with) a graphical user interface (GUI) for a user. The GUI helps to facilitate user login, data retrieval, and image creation and saving. Creation is defined broadly to include any alteration to an existing image, or generation of a new image. Initially, a user is requested to enter a password or pass code to interact with database **14**. After a successful log in, user access is preferably regulated based on security clearance. In other embodiments, permission levels or payment schedules are used to regulate access. An image, and related metadata, files, etc., should only be accessible when security access is permitted. In one embodiment, an image is selected from a directory, and the selected image is examined for watermarks. A watermark is extracted and security bits are determined. The security bits are validated against a corresponding security access allowed for the logged-on user. A user is permitted to access (e.g., retrieve, open, or edit) the image if she has an appropriate clearance. In an alternative arrangement, a database is queried to determine the security level required for all (or a subset of all) possible images in a directory or list. Only those images corresponding to the user's security clearance (or permission) are presented as options to open for the user. Even the names of the images can be screened from a user if her security clearance is insufficient.

[0050] The interface also facilitates communication in a normal image editing and creation processes. Preferably, the interface will be invoked as part of a saving process.

[0051] The creation process typically involves determining a new image identifier. As discussed above, there are many ways to determine an image identifier. In one case, the interface queries the database **14** to obtain a new image identifier. The retrieved image identifier is embedded in the newly created image as a portion of a digital watermark. The embedded image is then saved in database **14**. Optionally, the database will signal that the save operation has been successfully completed. In the case of derivatives, the data-

base is preferably updated to indicate that the new image identifier is related (or linked) to the identifier of an original image.

[0052] In one embodiment, the above-mentioned steps (e.g., creating, watermarking, and saving) are considered a transaction, e.g., where all of the steps must be carried out for the transaction to be complete.

[0053] Sentry

[0054] Another aspect of the present invention is a gatekeeper module. With reference to FIG. **4**, a gatekeeper (or "sentry") **42** resides on network terminals **40** and **44**. Terminals **40** and **44** communicate, e.g., via a network, direct link, e-mail, etc. Sentry **42** monitors the flow of digital watermarked images and related information by extracting digital watermark identifiers or embedded security information from transmitted images. The sentry **42** can compare extracted information against user (or terminal) security clearance information. In one embodiment, sentry is an independent software module, although sentry **42** may be incorporated into other software components (e.g., applications, operating system, etc.) of a network terminal **40** and **44**. Sentry **42** monitors and controls the flow of images at various points in a network system. Such activity is logged (e.g., recorded, stored, etc.) in database **46**. To monitor an image transmitted from user terminal **40** to user terminal **44**, sentry **42***a* decodes an embedded watermark identifier from an image to be transferred (step S**10**, FIG. **5**). The identifier, destination address, and optionally a date/time stamp are communicated to database **46** (step S**12**), where such information is recorded as a data record (or file, log, table, database entry, history, etc.) as in step S**14**. Preferably such transmission activity is associated with the unique identifier of the transferred image.

[0055] Sentry **42** is also gatekeeper in that it analyzes whether a user's security or permission level is sufficient to receive a watermarked image into or from a workstation (e.g., whether terminal **44** can receive the image transmitted from terminal **40**). Sentry **42***b* preferably includes watermark-decoding software, which extracts unique identifiers (and any security bits) from watermark images (step S**20**, FIG. **6**). If the security level of an image is stored in a database, sentry **42***b* queries the database with the identifier to determine the required access level. Or if the watermark includes security bits, then sentry **42***b* determines an access level directly from extracted security bits. Sentry **42***b* determines whether the user's security clearance sufficiently corresponds with the received image's clearance requirements (step S**22**). If so, sentry **42***b* allows terminal **44** to receive and open the subject image (step S**24**). If not, sentry **42***b* denies terminal **44** access to the image (step S**26**). In either case, sentry **42***b* preferably communicates such information to database **46** (step S**28**). For example, sentry **42***b* records whether the image is passed to terminal **44**, or whether the image is denied. (As an optional function, sentry **42***b* notifies terminal **42** regarding the delivery status of the image.).

[0056] Preferably, sentry **42** does not performed the function of managing the relationship between images and their derivatives, as this is the function of the file save software associated with the image editing application. However, in one embodiment, sentry **42** is combined with an application interface.

[0057] Sentry **42** can be deployed in a number of ways. In one embodiment, sentry **42** is integrated (or stored, or connected) to a workstation or server in such a way that all image data must first pass through the sentry **42**. In another embodiment, sentry **42** includes a separate hardware (or hardware/software) device inserted between a network (or network connection) and a user terminal. As such, sentry **42** decodes watermarks and intercepts passwords from image traffic before the user terminal receives the image, or directly after transmitting an image.

[0058] In another embodiment, e.g., in a TCP/IP environment, a sentry **42** is deployed as software within a TCP/IP stack in the user station or server. In yet another embodiment, a sentry is incorporated in (or called by) an image-handling program's open, save and close operations.

[0059] When used in connection with a database history or other record, sentry **42** provides efficient tracking and tracing. Since the history file reveals each use (and printing, transmission, etc.) of a watermarked image, the image can be efficiently tracked as it passes from terminal to terminal, or from database to terminal, etc.

[0060] Fragile Watermarks

[0061] Some images may include at least two watermarks. A first watermark includes a unique identifier, as discussed above. This identifier allows database inquires and association as discussed above. A second watermark can be applied prior to printing, faxing, etc. This second watermark preferably includes a so-called fragile watermark. That is, it is designed to be lost, or to degrade predictably, when the data set into which it is embedded is processed in some manner. (Fragile watermark technology is disclosed, e.g., in application Ser. Nos. 09/234,780, 09/433,104, 09/498,223, 60/198,138, 09/562,516, 09/567,405, 09/625,577, 09/645,779, and 60/232,163.).

[0062] Once an image is printed, it then includes both the first and second watermarks. If the image is subsequently scanned back into a digital form, e.g., via a scanner, photocopier, web cam, digital camera, etc., the fragile watermark is corrupted (or destroyed) in a foreseeable manner. Printed copies can be tracked and traced accordingly. For example, a photocopied image is scanned into a digital form. The first watermark is used to identify the image and retrieve an image history (e.g., as created by a sentry or other logging method). Since the fragile watermark is destroyed (or predictably degraded) in the copy process, the photocopy is determined to be an unauthorized copy. The history log can be used to determine which user, or user terminal, printed the copy.

CONCLUSION

[0063] Watermarks can be applied to any data set (e.g., an image, map, picture, document, etc.) for forensic tracking purposes. This is particularly useful where several copies of the same data set are distributed through different channels (e.g., provided to different users). Each can be "serialized" with a different identifier, and a record can be kept of which numbered data set was provided to which distribution channel. Thereafter, if one of the data sets appears in an unexpected context, it can be tracked back to the distribution channel from which it originated.

[0064] In an alternative embodiment, with reference to FIG. **1**, a digital watermark embedder is included in aerial

platform **11**. The aerial embedder embeds images (e.g., after or during capture) and relays such to ground station **12**. In yet another embodiment, an image is digitally watermarked downstream from ground station **12**, such as in a user terminal, or an embedder associated with the databases **14** and/or **15**.

[**0065**] Although not belabored, artisans will understand that the systems described above can be implemented using a variety of hardware and software systems. One embodiment employs a computer or workstation with a large disk library, and capable database software (such as is available from Microsoft, Oracle, etc.). The watermarking and database operations can be performed in accordance with software instructions stored in the disk library or on other storage media, and executed by a processor in the computer as needed. (Alternatively, dedicated hardware, or programmable logic circuits, can be employed for such operations.)

[**0066**] The various section headings in this application are provided for the reader's convenience and provide no substantive limitations. The features found in one section may be readily combined with those features in another section.

[**0067**] To provide a comprehensive disclosure without unduly lengthening this specification, the above-mentioned patents and patent applications are hereby incorporated by reference. The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this application and the incorporated-by-reference patents/applications are also contemplated.

[**0068**] It should be appreciated that the present invention is not limited to managing satellite and other aerial imagery. Indeed, other imagery may be managed with the present invention. Also, the present invention encompasses a "non-secure" type of system. In one such embodiment, watermark identifiers are used to link images and/or related information. A security or permission level is not required in such a system.

[**0069**] In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are illustrative only and should not be taken as limiting the scope of the invention. Rather, we claim as our invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof.

What is claimed is:

1. A method comprising:

receiving media including digital watermarking embedded therein through alterations to data representing the media, the digital watermarking including at least a first plural-bit identifier;

analyzing the media to obtain the plural-bit identifier;

communicating the plural-bit identifier to a remote database, the remote database including a plurality of usage rights indexed therein, the usage rights including a required security clearance associated with the plural-bit identifier;

receiving information indicating the required security clearance from the remote database;

obtaining information indicating a user's security clearance level;

determining whether to allow access to the media by the user based at least in part on whether the information indicating a user's security clearance level corresponds with the received information indicating the required security clearance.

2. A method of maintaining images in a database, wherein a first image includes a digital watermark embedded therein, the digital watermark comprising a first unique identifier, said method comprising:

storing the first image to be indexed by the first unique identifier;

storing information related to the first image; and

linking the first image and the related information by the first unique identifier.

3. A method according to claim 2 further comprising:

in the database, storing at least a second image and linking the first image and the second image with the first unique identifier.

4. A method according to claim 3, wherein the second image comprises a derivative of the first image.

5. A method according to claim 4, wherein the second image includes a digital watermark embedded therein, the digital watermark comprising a second unique identifier, and wherein said method further comprises linking the second unique identifier to the first unique identifier.

6. A method according to claim 4, wherein the related information comprises a history of the image.

7. The method according to claim 6, wherein the history comprises at least one of user usage, creation time, transmission, printing, and image checkout.

8. The method according to claim 2, wherein the database comprises a plurality of databases.

9. The method according to claim 2 wherein the related information comprises at least one item of information selected from a group comprising: metadata, location, date, permission level, security access levels, analyst comments, notes, files, and past usage information.

10. A method to monitor images in a system, the system comprising at least a first user terminal to communicate with a second user terminal and with a database, the images comprising at least a first image digitally watermarked to include a first identifier, said method comprising:

determining a security level associated with the first image;

comparing the first image security level with a user security level; and

allowing access to the first image based on a result of said comparing.

11. The method according to claim 10, further comprising recording a transmission in the database of the first image from the first user terminal to the second user terminal.

12. The method according to claim 10, wherein said determining comprises:

decoding the digital watermark to determine the first identifier; and

interrogating the database with the first identifier to retrieve the security level.

13. The method according to claim 10, wherein said first image's digital watermark includes security level data, and wherein said determining comprises decoding the digital watermark to determine the security level.

14. The method according to claim 10, wherein the user security level comprises at least one of a security level for a user and a security level for a user terminal.

15. The method according to claim 14 wherein when the result is a match between the first image security level and the user security level access is allowed.

16. The method according to claim 15 wherein the match indicates that the user security level is equal to or greater than the first image security level.

17. The method according to claim 15, further comprising recording access to the image.

* * * * *