NASA CASE NO. NPO-19108-1-CU

PRINT FIG. 3a, b, c,

NOTICE

The invention disclosed in this document resulted from research in aeronautical and space activities performed under programs of the National Aeronautics and Space Administration. The invention is owned by NASA and is, therefore, available for licensing in accordance with the NASA Patent Licensing Regulation (14 Code of Federal Regulations 1245.2).

To encourage commercial utilization of NASA-Owned inventions, it is NASA policy to grant licenses to commercial concerns. Although NASA encourages nonexclusive licensing to promote competition and achieve the widest possible utilization, NASA will consider the granting of a limited exclusive license, pursuant to the NASA Patent Licensing Regulations, when such a license will provide the necessary incentive to the licensee to achieve early practical application of the invention.

Address inquiries and all applications for license for this invention to NASA Patent Counsel, NASA Management Office-JPL, Mail Code 180-801, 4800 Oak Grove Drive, Pasadena, CA 91109-8099.

Approved NASA forms for application for nonexclusive or exclusive license are available from the above address.

Serial Number: 08/159,980

Filed Date: November 24, 1993 NMO-JPL

January 13, 1994

DIGITAL CAMERA WITH APPARATUS FOR AUTHENTICATION OF IMAGES PRODUCED FROM AN IMAGE FILE

Inventor: Gary L. Friedman

JPL Case No. 19108
Nasa Case No. NPO-19108-1-CU

Contractor: Jet Propulsion Laboratory

November 24, 1993

AWARDS ABSTRACT

The invention relates to a digital camera equipped with apparatus for enabling an image file produced by the camera to be authenticated.

FIG. 1 is a block diagram illustrating prior-art public key encryption technology and **FIG. 2** is a block diagram illustrating the prior-art method of producing and using a digital signature in a system having a private key and a corresponding public key.

In the present invention, illustrated in **FIG. 3a**, a system **10** comprising a digital camera **11** equipped with a processor **12** for authentication of images produced from an image file taken by the digital camera is provided. The digital camera processor **12** has embedded therein a private key unique to it, and the camera housing has a public key that is so uniquely based upon the private key that digital data encrypted with the private key by the processor **12** may be decrypted using the public key. The digital camera processor comprises means **12a** for calculating a hash of the image file using a predetermined algorithm, and second means **12b** for encrypting the image hash with the private key as shown in **FIG. 3b**, thereby producing a digital signature. The image file and the digital signature are stored in suitable recording means **12c** so they will be available together. Apparatus for authenticating at any time the image file as being free of any alteration shown in **FIG. 3c** uses the public key for decrypting the digital signature **22**, thereby deriving a secure image hash identical to the image hash produced by the digital camera and used to produce the digital signature. The apparatus calculates from the image file an image hash **21** using the same algorithm as before. By comparing this last image hash with the secure image hash **23**, authenticity of the image file is determined if they match, since even one bit change in the image hash will cause the image hash to be totally different from the secure hash. **FIG. 4** illustrates a colored border of an image file from a digital camera which includes pertinent information on camera parameters at the time a digital image is taken and the public key.

The novelty of the invention resides in the use of an embedded private key that may be known only to the camera manufacturer until fabrication is complete. The public key derived from the private key is then published (put on the camera housing and colored border of the image frame) for subsequent use at any time to authenticate the image file used to reproduce an image of a photographed scene.

Serial No. 08/159,980
Filing Date November 24, 1993
Contract No. NAS7-918
Contractor: Caltech/JPL
Pasadena, CA 91109-8099

JPL Case No. 19108
NASA Case No. NPO-19108-1-CU
F93183

Patent Application

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.

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

At one time, photographs were regarded as a medium that "never lies." However, the inherent trustworthiness of the photograph has 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) where the concept of an "original" image is no longer meaningful.

While a need for authenticating images 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 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 examine; furthermore, the digital image file produced by these cameras (as well as other digitally recorded artifacts, such as audio and video files) can be easily manipulated using sophisticated computers which make such manipulation easy and, as time goes on, 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 cleaning up "noise" and removing distracting backgrounds) 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 well-known adage that "a photograph does not lie" will become less credible.

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, or what the correct key is. The historic drawback to this secret key encryption scheme has been in the secure distribution of keys; key disclosure by the sender to the receiver must occur out-of-band, either transmitted via an expensive alternate path or arranged at some prior time, such as when sender and receiver were proximate.

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. Thus, public key encryption employs two different keys: a private key, which is held by the more security conscious party, 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 that could have been used to generate the resulting number.

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 would first make his/her public key known to the sender via any non-secure 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 send 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 eliminated. The tradeoff in this case is that, although only the recipient can read the message, anyone who obtains 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 this message. 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. The sender of a message generates a unique digital signature by hashing the message and using a private key to encrypt the hash. 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, unencrypted message so that a recipient may decrypt the digital signature and thus authenticate the message. A comparison of the decrypted hash and a hash of the message transmitted with the signature will readily show, if the decrypted hash and the

hash of the transmitted message do not match, 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. If the private key remains private, then only the private key holder can produce messages decipherable by the public key. Furthermore, it is extremely difficult to reverse-engineer the public key and ascertain the original private key. Without knowledge of the private key, a counterfeit message cannot be forged.

Digital signatures thus build upon these public key cryptographic techniques and allow a recipient to authenticate the contents of a plaintext message as well as the identity of the sender without obscuring the original message. Digital signatures are produced by creating a hash of the original plaintext 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 plaintext message as a separate block of data.

A "hash" is 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 practically 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 hash would produce a very different hash output. This advantage will become apparent in the present invention. Another advantage is that reverse

engineering a message so it will have a given hash value, and also make sense to the reader is virtually impossible. Thus, a digital signature can be created by encrypting the output of the hashing function using a sender's private key.

In the use of a digital signature, ***the original message is untouched***; only the message's hash is encrypted. This way, the original file can be read by all, yet each recipient may authenticate it by decrypting the message's unique digital signature using the public key. If the decrypted digital signature and an independent hash on the file in question match, both the integrity of the message and the authenticity of the sender can be 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 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.

STATEMENT OF THE INVENTION

An objective of the present invention is to provide a solution to the problem of authenticating digital images

reproduced from an image file, where the image file may be a single still image from a camera, a sequence of images from a digital video camera, or even a digital hologram or digital audio from a recording system. Authentication in this sense means to establish as worthy of belief that the image file has not been altered. The term "image file" is thus used herein to refer to the recorded file of a digital still camera, a digital video camera, a digital holographic camera system, or a digital audio recorder.

In accordance with the present invention, a digital camera 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 first means for 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 encrypting the hash with a unique private key embedded in second means (known to nobody except perhaps the manufacturer of the camera or this second means implemented, for example, as a programmed microprocessor) for which there is a known public key unique to the camera. The encrypted hash is stored along with the image file 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 from the true 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.

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. 3a illustrates a preferred application of the present invention to digital cameras.

FIG. 3b 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. 3c is a block diagram of a system for authenticating the file image from the digital camera of **FIG. 3a.**

FIG. 4 illustrates a colored border of an image from a digital camera.

DETAILED DESCRIPTION OF THE INVENTION

As applied to digital cameras, the objective is to provide a digital signature for an image file as it emerges from a 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. 3a:** the first is an all digital, industry standard format image file representing the captured image. The second would be an encrypted digital signature produced as shown in **FIG. 3b** by applying the camera's unique private key (embedded within the digital camera's secure microprocessor **12b**) to a hash of the captured image file, produced by hashing microprocessor **12a** for creating an image hash, thus producing the digital signature which, like the image file, may be recorded in the recorder **12c** of the digital camera system **10** or transmitted to a digital processor's memo-

ry. It is the responsibility of the user to keep track of both the image and digital signature files once they leave the camera **10** since both are required to authenticate the image.

Once the digital image file and the digital signature are generated and stored on a medium in the camera system and then transferred into a digital processor memory, or alternatively transmitted directly to a digital processing system, the image file's authenticity can be affirmed at any time thereafter by a decrypting system **20** shown in **FIG. 3c** using a public key taken from the camera name plate or the image's border. The public key can be freely distributed to users and certification authorities via conventional software distribution techniques. 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 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 decryptor **22** comprising a digital processing system using the public key 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 a 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 audio, digital video, or even digital hologram recording, reliance is made upon the accomplishments 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 audio cassette tape or the NTSC encoding on today video tape formats, or noncorrected digital formats such as the popular audio compact disc (CD), which is so unreliable that CD player manufacturers now utilize special techniques, such as "oversampling" to combat the problem of missed bits, introduce such a large number of errors upon playback which are normally imperceptible to the human viewer/listener, are unsuitable for the purposes of image authentication. Consequently, the present invention is directed to digital recording systems of all kinds such as digital audio, video and hologram recording for authentication of recorded files collectively referred to as image files. On the other hand, the claims appended hereto are to be construed to cover all recording means: a digital camera for image recording is used as an example to illustrate a preferred embodiment of the invention. The term "image

file" used for that example applies directly to the recorded file in other systems as well, such as digital audio recording systems.

Measures of Protection

The invention as described above is resistant to forgery attempts since the private key (which is known to nobody except possibly 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 pirate were to dissect the camera and replace the microprocessor chip with one containing a homebrew key, the digital signature produced thereafter would not be decryptable by any public key published by the manufacturer.

The advantages to 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 bad-faith amongst the parties involved need be created as a result of being challenged. But the mass distribution of the verification algorithm does carry one danger: it would be easy 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 can be easily obtained from multiple sources and a more reliable authenticity check made by a best two-out-of-three scheme. Alternatively, as a weak check, a digital signature and an image file known to have an altered image may be used to check the algorithm of the

authenticator 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 recording system (the digital camera in the example) could be called in to provide their own copies of the algorithm and the public key from their own list of public keys (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 colored 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. This would eliminate the possibility of compromise via 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 his own private key. Decoding these forgeries would require the use of a public key not generated by the manufacturer. Freely distributing updated public key lists would make it easy to identify and thwart such attempts.

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 and digital audio recorders as well, as noted hereinabove. 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 sound byte or video "take" is hashed, encoded and written at the time it is recorded, or in the case of continuous recording by a digital, audio or video recorder at the time each block is completed by using the technique of multiplexing between three sets of buffers; as one buffer is filled with a block of data, another is hashed, encrypted and recorded at a faster clock rate so that its algorithms are complete in time to record the digital signature before a multiplexer shifts functions amongst the three sets for the next block of data. Thus, with three sets of buffers A, B and C, assume A is receiving input, B is hashing and encrypting it, and C is recording. During the next block interval, the functions 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 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 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 camera's public key, the focusing distance of the lens at the time of exposure, a unique 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 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. The lens' focused distance and *f*/stop are there to help detect potential abuse of the camera: taking close-up pictures of a modified photo and trying to pass it off as an unaltered original.

Since all these textual data in the colored 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 saboteur will be able to crack 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 horsepower will be enough to render any given level of cryptographic protection obsolete.) If the discovered private key were then to be available to the user of the compromised camera (the camera having the corresponding public key (serial number)), it would allow the individual having 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 cameras, will still 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 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 then be designed to recognize, identify and authenticate all previous versions.

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 application in audio, video and holographic images may also benefit from it. Although it will always be possible to lie using a photograph by such time-honored techniques as false perspectives and misleading captions, the present invention will prevent the rapid development of very capable personal computers from increasing the incidence of altered images being passed off as authentic images.

F93183

18
~~20~~

DIGITAL CAMERA WITH APPARATUS FOR AUTHENTICATION OF IMAGES PRODUCED FROM AN IMAGE FILE

ABSTRACT OF THE DISCLOSURE

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 based upon the private key that digital data encrypted with the private key by the processor 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 at any time 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 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, since even one bit change in the image hash will cause the image hash to be totally different from the secure hash.

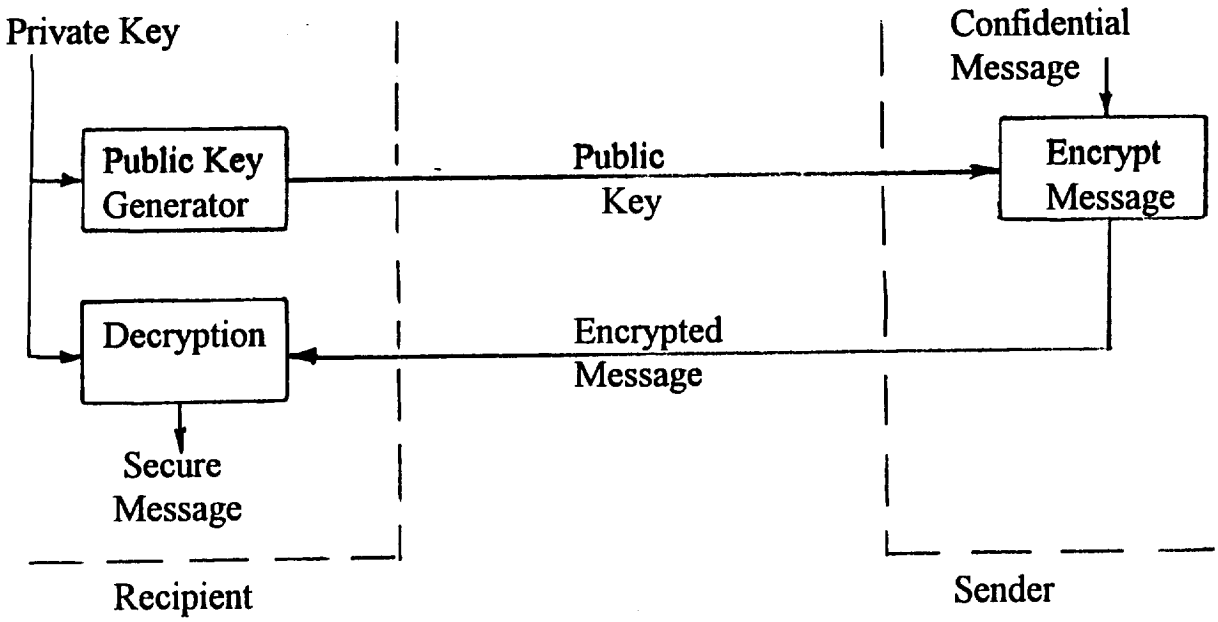

FIG. 1
Prior Art

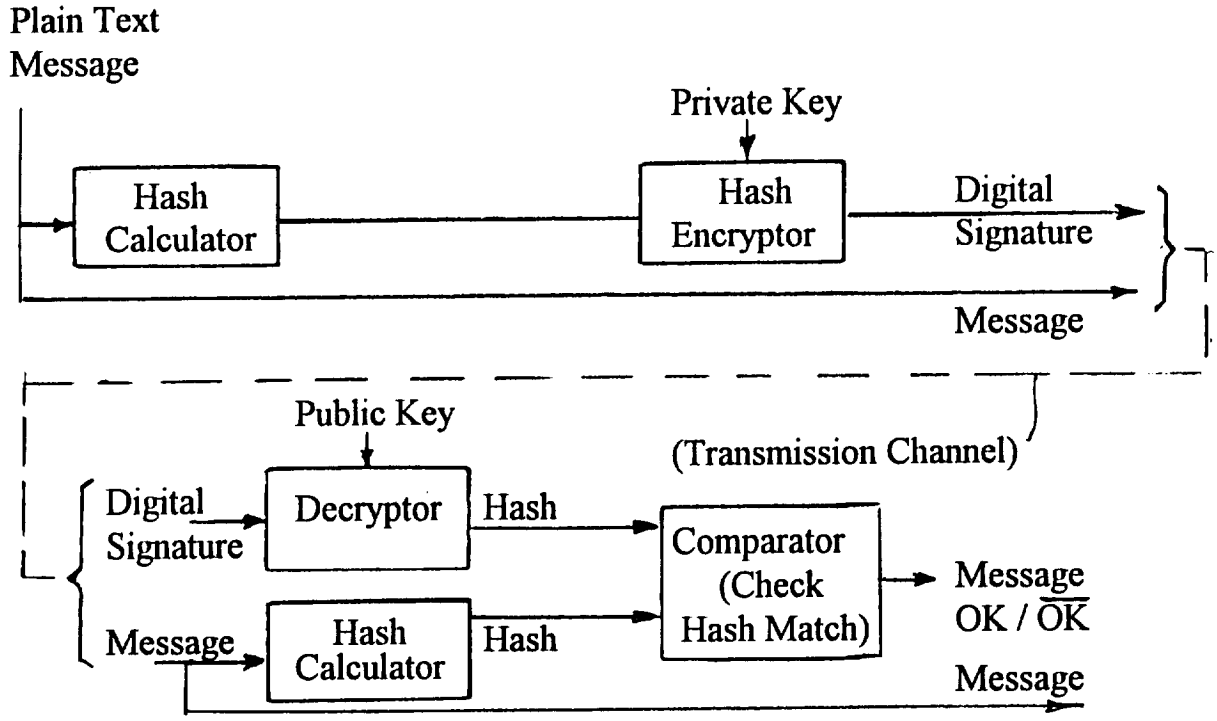

FIG. 2
Prior Art

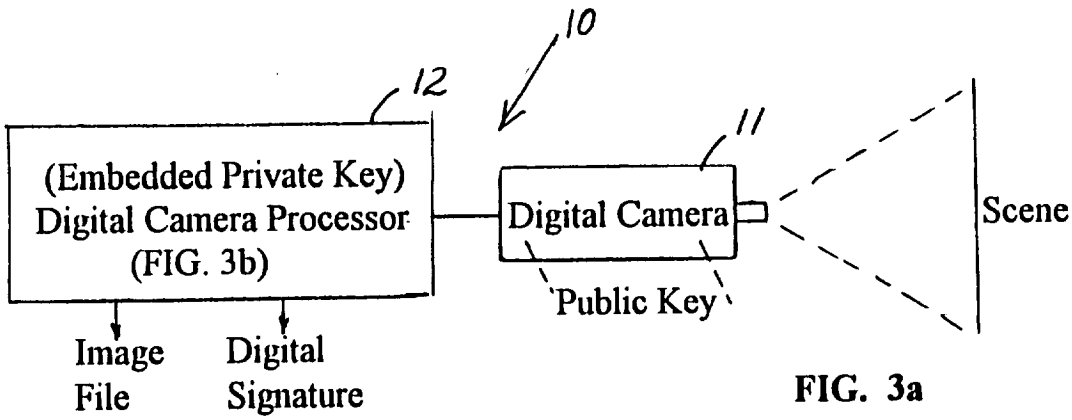

FIG. 3a

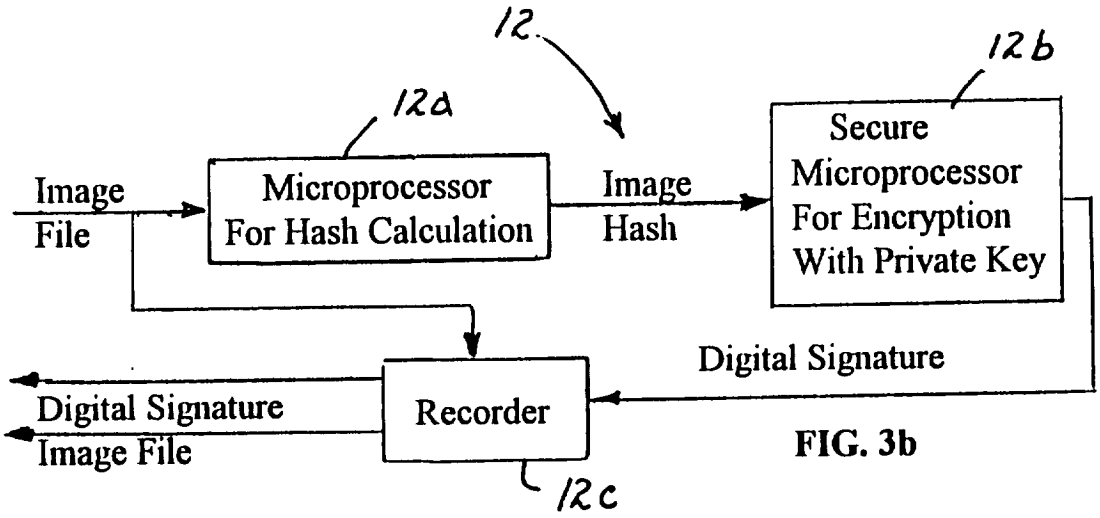

FIG. 3b

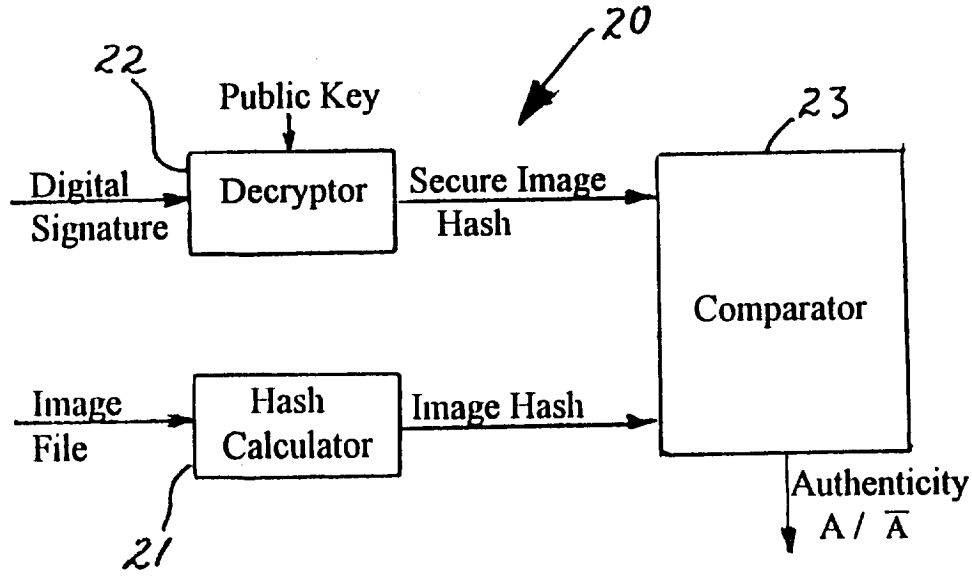

FIG. 3c

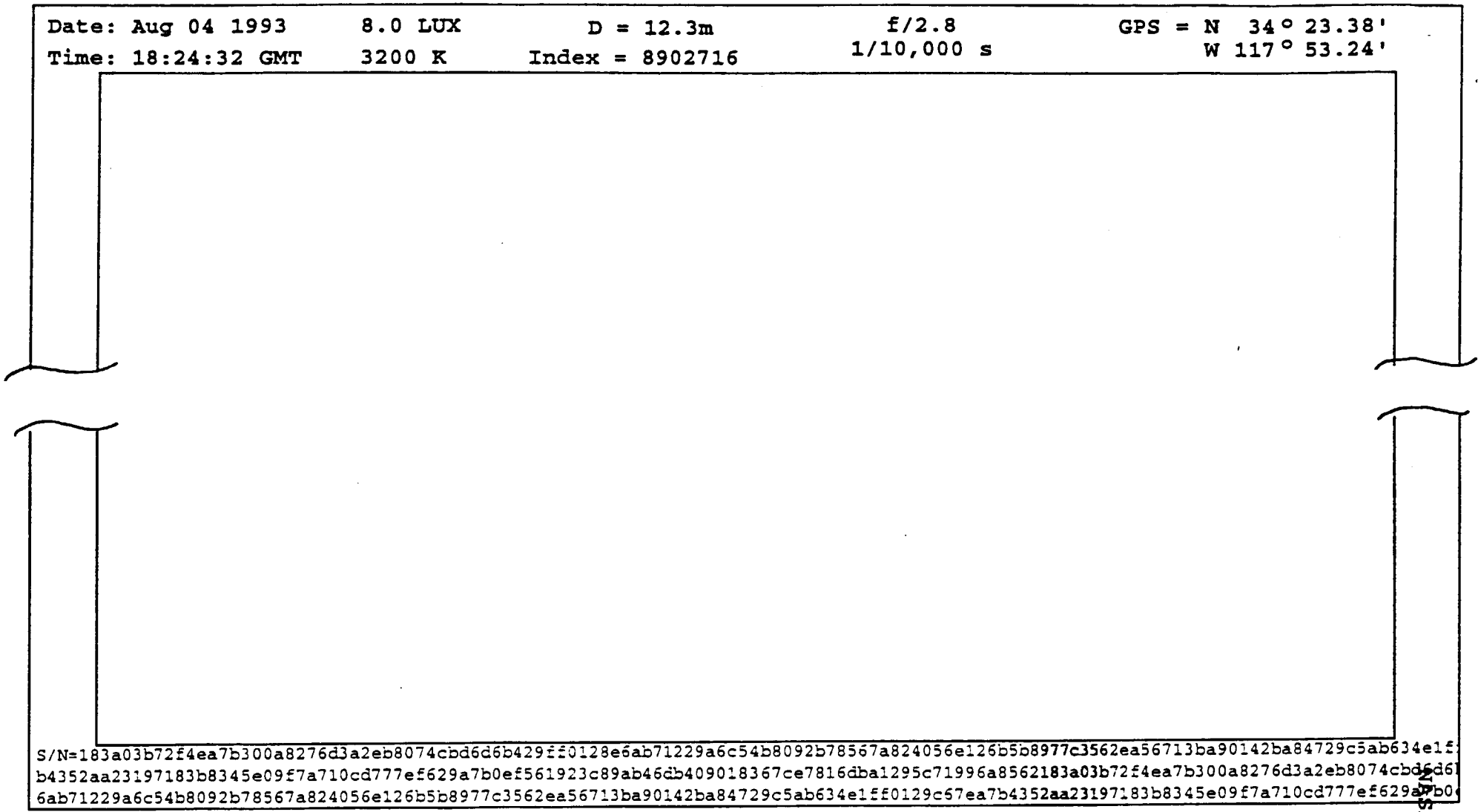
Date: Aug 04 1993
Time: 18:24:32 GMT
8.0 LUX
3200 K
D = 12.3m
Index = 8902716
f/2.8
1/10,000 s
GPS = N 34° 23.38'
W 117° 53.24'
S/N=183a03b72f4ea7b300a8276d3a2eb8074cbd6d6b429ff0128e6ab71229a6c54b8092b78567a824056e126b5b8977c3562ea56713ba90142ba84729c5ab634e1f
b4352aa23197183b8345e09f7a710cd777ef629a7b0ef561923c89ab46db409018367ce7816dba1295c71996a8562183a03b72f4ea7b300a8276d3a2eb8074cbd6d61
6ab71229a6c54b8092b78567a824056e126b5b8977c3562ea56713ba90142ba84729c5ab634e1ff0129c67ea7b4352aa23197183b8345e09f7a710cd777ef629a7b0
NASA NPO-19108-CU

FIG. 4