PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 12/14 — A1

(11) International Publication Number: **WO 00/00895**

(43) International Publication Date: 6 January 2000 (06.01.00)

(21) International Application Number: PCT/US99/10390

(22) International Filing Date: 11 May 1999 (11.05.99)

(30) Priority Data:
09/105,593 26 June 1998 (26.06.98) US

(71) Applicant: FOTONATION, INC. [US/US]; 199 California Drive, Millbrae, CA 94030 (US).

(72) Inventor: STEINBERG, Eran; 372 Douglass Street, San Francisco, CA 94114 (US).

(74) Agent: JAFFER, David, H.; Rosenblum, Parish & Isaacs, 15th floor, 160 West Santa Clara Street, San Jose, CA 95113 (US).

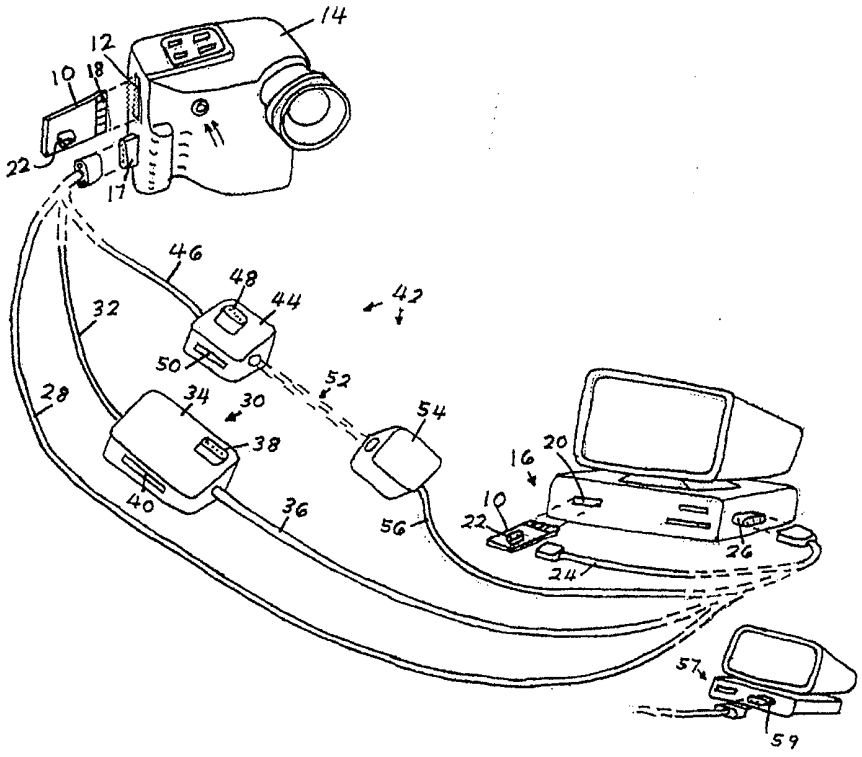
(81) Designated States: JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: SECURE STORAGE DEVICE FOR TRANSFER OF DIGITAL CAMERA DATA

(57) Abstract

A secure storage device (10) with the external dimensions of a PCMCIA, for securing data of a digital camera (14) at the acquisition stage. Original digital camera data is saved in the memory of the secure storage device which has the capability of performing one or more security functions, including encryption, creation of authentication file, adding data to the image data such as data included in an image header. The device prepares original authentication data from original digital camera data, and encrypts and stores both the original authentication data and the original image data. The use of the device includes downloading the original authentication data to a first computer (16), and encrypting original authentication data to a second computer. The second computer can be programmed with software whereby the encrypted original authentication data can by decrypted by a user having a key. The software then allows the user to prepare corresponding second authentication data from second image data of questionable authenticity. If the second authentication data is the same as the original authentication data, the questionable second image data is deemed to be an accurate copy of the original image data.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Specification

SECURE STORAGE DEVICE FOR TRANSFER OF DIGITAL CAMERA DATA

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates generally to digital still and video cameras and the transfer of data from a digital camera to a computer, and more particularly to an apparatus for transparently providing embedded security of data within a storage device and of securing data while being transferred from a digital camera to a computer.

Brief Description of the Prior Art

In many applications, photographic data needs to be guarded or i.e. secured against unauthorized viewing, modification or distribution. Negatives, positives and prints can be manipulated with some effort, and need protection when used to accurately document images. In such a case, the original negatives and prints are typically kept in locked facilities, with signed, sealed and witnessed chains of custody. The advent of digital cameras presents even greater security challenges. The concept of an original digital image is questionable, because digital data can be perfectly replicated. In addition, digital image data can be quickly and easily modified in a computer, rendering the data useless for evidentiary purposes. Currently, digital camera image data is downloaded either directly to a computer from a camera via some communication mechanism, or through a removable storage device, such as a PCMCIA card, etc. Upon downloading the data to a computer, the image data can be encrypted, or authentication data can be created to prevent an unauthorized person from

modifying the data. From this point on, a witnessed chain of custody of those persons with access to the decryption key can be maintained, greatly easing the security problem.

From the above description of the prior art, it is apparent that there is a need for a method and apparatus for securing camera data automatically prior to, or as part of downloading image data from a camera. Such a method and apparatus would greatly improve the security of digital camera data.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a method and apparatus for securing data from digital still and video cameras during the process of transferring the data from a camera to a computer.

It is a further object of the present invention to provide a secure storage device for digitally saving data from a digital camera.

It is a further object of the present invention to provide a method and apparatus for securing data from still and video cameras during the process of transferring data from a camera to a computer, wherein the securing process is undetected by or i.e. transparent to the camera, and therefore providing a method and apparatus that can be used with any digital camera.

It is a further object of the present invention to provide a secure storage and/or communication device that automatically encrypts loaded digital camera data.

It is another object of the present invention to provide an apparatus with dimensions and connectors in the form of a PCMCIA card that is accepted by a digital camera and a destination computer as a standard PCMCIA card, while performing the function of automatically securing loaded digital camera data.

It is a still further object of the present invention to

provide a secure storage and/or communication device that can be programmed with a security key, that automatically stores loaded original digital camera data, and prepares encrypted authentication data.

It is another object of the present invention to provide a secure storage and/or communication device that inserts information into loaded digital camera image data, i.e. performs fingerprinting.

It is a further object of the present invention to provide a secure storage and/or communication device that includes additional information along with the image data, i.e., provides annotations, such as the absolute time of acquisition, a unique and continuous image counter, and a unique image and device identification number.

Briefly, a preferred embodiment of the present invention includes a secure storage device with the external dimensions of a PCMCIA card, for securing digital camera data at the acquisition stage. Original digital camera data is saved in the memory of the secure storage device which has the capability of performing one or more security functions, including encryption, creation of an authentication file, adding data to the image data such as fingerprinting, and adding secure annotations such as separate data included in an image header. The device prepares original authentication data from original digital camera data, and encrypts and stores both the original authentication data and the original image data. The use of the device includes downloading the original image data to a first computer, and encrypted original authentication data to a second computer. The second computer can be programmed with software whereby the encrypted original authentication data can be decrypted by a user having a key. The software then allows the user to prepare corresponding second authentication data from second image data of questionable authenticity. If the second authentication data is the same as the original authentication data, the

questionable second image data is deemed to be an accurate copy of the original image data.

An advantage of the present invention is that it provides a method and apparatus for securing data while storing and transferring otherwise unsecured image data received from a digital camera for transfer to a computer.

A further advantage of the present invention is that it provides a method and apparatus for securing the chain of custody of digital data from cameras that would otherwise provide only unsecured image data.

Another advantage of the present invention is that by putting the security function in a removable storage device, the storage can be customized for a particular user with no need for special hardware on the camera or the PC, enabling the retrofitting of otherwise unacceptable cameras with appropriate security functionality.

A still further advantage of the method and apparatus of the present invention is that the processing provided is undetected i.e. transparent to the camera and to the computer, and as a result the method and apparatus can be applied to any digital camera, and also to a variety of other devices that utilize peer to host and peer to peer communication and/or removable storage.

IN THE DRAWING

Fig. 1 is a perspective view illustrating the use of the present invention to transfer data;

Fig. 2 is a block diagram showing the method steps of secure data transfer;

Fig. 3 is a block diagram of a secure storage device;

Fig. 4 is a block diagram of a secure data transfer device;

Fig. 5 illustrates the transfer of secure data by way of data encryption;

Fig. 6 illustrates the storage device for secure data

transfer through creation of authentication data;

Fig. 7 illustrates the process of a host computer for verifying image data authenticity through use of authentication data;

Fig. 8 shows a method of secure data transfer by way of fingerprinting and/or annotation; and

Fig. 9 illustrates the sending of secured data from a secure storage device to a first location, and public data to a second location.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring now to Fig. 1 of the drawing, the method and apparatus of the preferred embodiment of the present invention is illustrated. The preferred embodiment includes an electronic digital signal processing apparatus, referred to as a secure storage device 10, and configured to physically engage with a PCMCIA card slot 12 of a prior art digital camera 14. Although the camera 14 shown is typical in appearance to a still camera, the method and apparatus also applies to motion picture/video cameras.

According to the method of the present invention, the device 10 is initially programmed to receive data from a digital camera, without the need of a password/key from the camera, and to perform the required processes to secure the data from the camera 14. The initial programming of device 10 can be either fixed, one time programming of a ROM, and/or it can be a program downloaded by a user from a PC such as PC 16. This programming data, as well as additional data, can be loaded into device 10 through the PCMCIA terminal 18 from a corresponding PCMCIA slot 20 in the PC 16. Alternatively, the device 10 can receive data through an input port 22 connected for example with a cable assembly 24 to a compatible port 26 of PC 16. The device 10 can be programmed to perform any of a variety of processes to secure the data, including encryption of image data, and/or creation of encrypted image

authentication data, or watermarking, etc.

In operation, the programmed device 10 is inserted in slot 12 of the still/video camera 14. When the device 10 receives data from the camera 14, it performs the programmed operations and stores the data. The device 10 is then removed from the camera 14 and inserted into the PCMCIA slot 20 of the computer 16. The device 10 is configured so that the PC 16 recognizes the device 10 as a regular storage device with readable files on the file system level without the need for presenting a password. The secure data is then transferred from the device 10 to the computer 16. In order for a user to view encrypted data, the computer 16 must be programmed to decrypt the data, generally in response to entry of a password.

Referring again to Fig. 1, according to the prior art, a digital camera 14 is connected to a computer 16 by way of a direct cable connection indicated by line 28 making a direct cable connection from the camera connector 29 to the PC connector 26. In this manner, unsecure camera data is directly transferred to a PC 16. An unauthorized user could then easily modify the data with the PC 16. The method and apparatus of the present invention solves this problem by first transferring the camera data to the secure storage device 10, which automatically secures the data. Two alternate embodiments of the present invention are also shown in Fig. 1.

A first alternate embodiment includes a secure data transfer device 30 having an input cable assembly 32 for making a connection from the camera 14 connector 29 to a security device 34. The security device 34 performs the same or similar operations as those discussed in reference to device 10 for securing the image data, and outputs the data to the PC 16 through an output cable 36, which in operation is connected to connector 26 of PC 16. The device 34 is programmable, and can receive additional data in the same manner as device 10, by connection to a computer through either cable assembly 32 or 36, or alternatively through a connector 38, or by way of a

PCMCIA card through a PCMCIA card slot 40.

The second alternative embodiment, also shown in Fig. 1, includes a wireless secure data transfer device 42, including a security device 44 that can be connected to a camera 14 by way of a cable assembly 46. The device 42 is programmable and receives additional data either from a PC through cable assembly 46 or connector 48, or by way of a PCMCIA card through slot 50. The device 44 includes a transceiver having a modulated infrared transmitter portion for generation of an infrared signal 52 for transmission of data to an infrared transceiver 54 which receives and demodulates the signal, and outputs the data to the computer 16 through a cable assembly 56. The transceiver properties of device 44 and transceiver 54 in addition allow for programming and other data to flow from PC 16 to device 44 through the wireless infrared connection.

In all of the above embodiments, the devices 10, 30 and 42 present a standard interface to the camera 14 and PC 16. From the camera's point of view, the communication appears as if a direct connection is made to the PC. Similarly, the PC observes a connection that appears to be directly to the camera. This feature of transparency of the devices 10, 30, 42 allows the apparatus and method of the present invention to apply to any digital camera and any PC that is programmed to receive digital camera data. The security is performed inside the device 10, 30, 42 and has no effect on the camera or PC.

The computer 16 of Fig. 1 represents a destination to which the camera data is being transferred. Although a PC is illustrated, this destination can be any computerized network, system, etc. capable of receiving the data. Fig. 1 also shows a second destination 57 with a data input connection 59. The second destination 57 is shown to illustrate an important alternate embodiment of the method of the present invention, wherein a user can hook the output of device 10, 30, or 42 to a first destination 16 to download a first set of data, for example encrypted authentication data, and then to the second

destination 57 to download a second set of data, which for example could be authenticated image data.

Fig. 2 shows the basic process in block form. Block 58 includes the operation of a digital camera writing original digital camera data to a secure storage device without the need for presenting a password. This data is received by the storage device and secured (block 60), a process requiring a pre programmed key. The storage device then writes the secured data (block 62), again without requiring the receipt of a password, which is read by the computer (block 64). In this operation it is assumed that the user has loaded the required operating software into the computer. The user must then present a password/key to the computer in order to decrypt the secure data or perform an authentication operation (block 65).

It is important to point out here that the storage device described herein presents an external behavior/interface to the camera that appears to the camera to be the same as the prior art devices into which the camera is designed to download data. A major distinction between the prior art storage devices designed and used for digital cameras and the secure device of the present invention is that the disclosed device upon receiving data/information, performs operations to secure the data. This is done without requiring a password or key from the camera, which is an important feature of the present invention. Similarly, a computer can receive the secure data from the storage device without presenting a password/key. Once the secure data is loaded in the computer, a key must be presented in order to decrypt the secure data.

The advantage of this method is that no special programming or apparatus, other than the secure storage device, is required in order to securely transfer data from a conventional prior art digital camera to a computer.

The preferred external physical configuration of the secure storage device is that of a standard PCMCIA card, for example device 10 of Fig. 1 without the connection 22. In this

configuration, neither a user nor the camera nor a computer can distinguish the secure storage device from a standard PCMCIA card. The device accepts data from a camera, and sends data to a computer using standard protocol as if the device is a regular PCMCIA card. The only difference is that the data is secured through any of various means which will be described in the following specification, such as encryption, authentication, etc. A user's only clue concerning the unique nature of this device is that encrypted data loaded into a computer from the device will not be intelligible until decrypted, a process requiring special software in the computer, including a password and/or key. A point of novelty illustrated in Fig. 2 is that no password or key is required either to download data from the camera to the device, or from the device to a computer, as indicated in blocks 58, 62 and 64. This method allows maximum security of data, while allowing use of a standard digital camera and computer for all phases except the find step (block 65), wherein the user must load appropriate software with a key into the computer for decryption of the encrypted data.

Other physical embodiments of the secure storage device are as illustrated and discussed in reference to Fig. 1. In addition, the device 10 can alternatively be a SSFDC (Smart Media) card, or flash card, etc.

Fig. 3 illustrates typical circuit blocks required within the device 10. The connector/connection 18 passes data from the camera 14 to a card interface 66 providing the necessary protocol for communication with the camera. Bus line 68 interconnects the various circuit blocks as required. This is a memory 70,which can include a EEPROM and/or a ROM and RAM as required in a particular design. The card storage block 72 indicates the use of a floppy disk, or mini disk, etc for retaining the data for storage and transfer to a computer. Card controller 74 performs the standard/usual card operations, with additional processes accomplished by processor 76, which

preferably includes a clock 78, counter 80, and facility for receiving additional data (block 82) from a PC through either of connectors 18 or optionally through PC interface controller 84 from connector 22. The processor also performs image processing activity 86 including security process 88. The power supply 90 is included as optional in design, including a clock, for example, or where power cannot be obtained from the camera and computer.

Fig. 4 illustrates typical circuit block functions for devices 30 and 42. Device 30 includes cable connector assemblies 32 to a camera and 36 to a computer, and security device 34. Device 42 includes the cable connector assemblies 46 and 56, and security device 44 which includes the circuitry in security device 34 with transceiver circuitry 54 added, and the separate transceiver 54.

The device 34 circuitry includes a camera connection controller 92, power supply 94, memory 96, a removable storage controller 98 providing interface to card connection 50, a PC interface controller 100 providing interface to cable connector assemblies 48 and 36, a processor 102 with a clock 104, counter 106, additional data 108, image processing 110 and a security engine 112. The storage 114 is optional for the data transfer devices 30 and 42, and is for storing the data to be transferred from a camera to a computer, and can be a floppy disk, mini disk, etc. Since the use of the devices 30 and 42 preferably involves connecting to both the camera and destination at the same time, data can normally be transferred quickly enough so that memory 96 can provide adequate storage/buffering. If applications require longer storage, the optional storage 114 can be included in the design.

Fig. 5 illustrates the processes of the secure storage devices 10,30,42 for encryption of original digital camera data. According to the process, the storage device is initially programmed with a security key (block 126). This operation is done as an initial set-up of the device, prior to

it's normal usage. This key programming can be a permanent setting, or it can be programmable. With the devices 10, 30, 42 ready for normal use, it is then connected to a camera and receives original digital camera data (block 128). The device then encrypts the original digital camera data (block 130). Following this, the device is removed from the camera and connected to a computer loaded with compatible software. The device 10, 30, 42 then writes the data to a computer (block 132). A user knowing the security key can then operate the computer to decrypt the encrypted data (block 134). As explained in reference to the method indicated in Fig. 2, the device 10, 30, 42 does not require receipt of a password/key to receive data from a camera, or to download data to a computer. The key is used in the encryption process and is only a factor when a user desires to view the original data through use of the computer.

A secure storage device can also be programmed to create authentication data. This is illustrated in Fig. 6. As in the case of Fig. 5, the storage device is initially programmed with a security key (block 136) prior to use of the device. The device is then connected to a camera to receive original camera data (block 138). Authentication data is then created within the storage device from the original camera data and then encrypted (block 140).

Any person can then download the camera data, i.e. cause the storage device to write the camera data (block 142), and authentication data/file (block 144) to a computer. This completes the function of the storage device. The user can then proceed to use the computer as indicated in Fig. 7 to verify the authenticity of a set of questionable data. The user first uses appropriate software and the key to create verification authentication data from the questionable image data file (block 146), and decrypts the encrypted original authentication data (block 148). The two sets of data are then compared (block 150). If they are the same, the questionable

image data is considered valid, i.e. an accurate replica of the original image data. If the two sets are different, the questionable data is confirmed to be different from the original.

Fig. 8 illustrates two similar processes called "fingerprinting" and "annotating". Fingerprinting is a process wherein additional information is visibly or invisibly inserted into the image data itself. Examples of additional information that can be added include the camera serial number, date and time, unique counter, image storage ID, and any textual information that is downloaded to the storage device prior to receiving the camera image data. The process of annotation is similar to fingerprinting, except that the information is placed in a non-image area such as the header, rather than in the image data. Referring to Fig. 8, the storage device is connected to a computer and the required data is inputted, i.e. downloaded (block 152). This can be done through connection 18 for a PCMCIA card configured device 10, or through connector 22 of the alternative device 10. Device 42 is configured as indicated in Fig. 4 to receive data through port 48 or through cable assembly 46 or through cable assembly 50 from a PC, or through port 56 from a PC, or through port 50 from a PCMCIA card. Similarly, device 30 is configured to receive data alternatively through cable assembly 32 or 36, or connector 38 from a PC, or through port 40 from a PCMCIA card. The storage device is then connected to a camera and receives camera data, i.e. camera data is downloaded (block 154). The device then performs programmed processes of either fingerprinting the data or annotating the data file (block 156) depending on the specific programming of the storage device. The storage device is then removed from the camera, connected to a computer, and the data is written, i.e. downloaded to the computer (block 158). As explained above, this is all done without the presentation of a password or key from the camera or computer. Once the data is in a computer, however, the

original data or authentication requires submission of a password/key.

In some cases, it is preferred to keep a signature file or authentication file in a secure, private location, and allow public access only to an authenticated image. These processes are illustrated in Fig. 9, wherein image data is downloaded from a camera 160 to a secure storage device 162, which performs the required security functions. The device 162 then downloads the image security data to secure location 164, and an authenticated image to public access 166.

Although the present invention has been described above in terms of a specific embodiment, it is anticipated that alterations and modifications thereof will no doubt become apparent to those skilled in the art. It is therefore intended that the following claims be interpreted as covering all such alterations and modifications as fall within the true spirit and scope of the invention.

What is claimed is:

CLAIMS

1. A method of securing digital camera data comprising:
   (a) downloading digital camera data from a digital camera to a secure storage device; and
   (b) creating secure data within the secure storage device by performing digital processing related to the digital camera data.

2. A method as recited in claim 1 wherein the secure device is responsive to the same protocol as an unsecure device and as a result the secure device is transparent to the camera, whereby the camera responds to the secure device as if it were an unsecure storage device.

3. A method as recited in claim 2 further comprising downloading the secure data from the secure device to a host computer, wherein the secure device is responsive to the same protocol as an unsecure device and as a result the secure device is transparent to the computer, whereby the computer responds to the secure device as if it were an unsecure storage device.

4. A method as recited in claim 1 further comprising:
   (a) loading the secure device with additional data; and
   (b) storing the additional data in the secure device.

5. A method as recited in claim 4 wherein the secure data includes annotations taken from the additional data and added to a non-image area.

6. A method as recited in claim 4 wherein the additional data is downloaded from a computer.

7. A method as recited in claim 5 wherein the additional data is downloaded from a camera.

8. A method as recited in claim 4 wherein the additional data is

encrypted.

9. A method as recited in claim 1 further comprising a first step of inputting a security key to the secure storage device.

10. A method as recited in claim 1 wherein said secure data is encrypted data.

11. A method as recited in claim 1 wherein the secure data includes encrypted digital camera data.

12. A method as recited in claim 1 wherein the secure data includes encrypted authentication data.

13. A method as recited in claim 4 wherein the secure data includes fingerprinted digital camera data, and the fingerprinted digital camera data includes additional data added to the digital camera data.

14. A method as recited in claim 10 further comprising:

(a) interconnecting the secure storage device to a computer; and

(b) decrypting the secure data within the computer.

15. A method as recited in claim 7 wherein the additional data includes the time and date of taking a picture.

16. A method as recited in claim 4 wherein the additional data includes the time and date of writing the data to the secure storage device.

17. A method as recited in claim 4 wherein the additional data includes data indicating a unique single step image counter number for the digital camera data in the secure storage

device.

18. A method as recited in claim 4 wherein the additional data is data indicating a unique device identification.

19. A method as recited in claim 1 wherein the camera is for taking still pictures.

20. A method as recited in claim 1 wherein the camera is a video camera.

21. A method of securing digital camera data comprising:
(a) downloading camera data through an input means to a security communication device, the security communication device having an output means connected to a first destination;
(b) creating secure camera data within the security device; and
(c) transferring the secure camera data from the security device through the output means to the first destination.

22. A method as recited in claim 21 wherein the first destination is a computer.

23. A method as recited in claim 22 wherein a transmission protocol for the downloading is the same protocol as used in standard communication to and from the camera and as a result the secure device is transparent to the camera and the computer, whereby the computer and the camera respond to the secure communication device as if it were an unsecure communication device.

24. A method as recited in claim 21 wherein the input means includes first cable means for connecting the camera to the security device.

25. A method as recited in claim 21 wherein the security device includes

(a) first transceiver means for sending and receiving a radiated signal carrying data; and

(b) second transceiver means for sending and receiving a radiated signal for transmission of the data through the output means to and from the first destination.

26. A method as recited in claim 21 wherein the output means is a cable connecting the security device to the first destination.

27. A method as recited in claim 26 wherein the security communication device is responsive to the same protocol as an unsecure device and as a result the security device is transparent to a digital camera and to a computer, whereby a computer and a camera respond to the security device as if it were an unsecure device.

28. A method as recited in claim 21 wherein the camera is a still camera configured for taking still pictures.

29. A method as recited in claim 21 wherein the camera is a video camera.

30. A method as recited in claim 21 further comprising:

(a) loading the security device with additional data; and

(b) storing the additional data in the secure device.

31. A method as recited in claim 30 wherein the secure data includes annotations taken from the additional data, and the method further comprising adding the annotations to a non-image area.

32. A method as recited in claim 30 wherein the additional data is downloaded from a computer.

33. A method as recited in claim 30 wherein the additional data is downloaded from a camera.

34. A method as recited in claim 30 wherein the additional data is encrypted data.

35. A method as recited in claim 21 further comprising a first step of inputting a security key to the secure storage device.

36. A method as recited in claim 21 wherein the secure data is encrypted.

37. A method as recited in claim 21 wherein the secure data includes encrypted said digital camera data.

38. A method as recited in claim 21 wherein the secure data includes encrypted authentication data.

39. A method as recited in claim 30 wherein the secure data includes fingerprinted digital camera data, and the fingerprinted digital camera data includes additional data added to the digital camera data.

40. A method as recited in claim 21 further comprising:
decrypting the secure data within the first destination.

41. A method as recited in claim 33 wherein the additional data includes a time and date of taking a picture.

42. A method as recited in claim 30 wherein the additional data includes a time and date of downloading the camera data to the security device.

43. A method as recited in claim 30 wherein the additional data includes data indicating a unique single step image counter number for the digital camera in the security device.

44. A method as recited in claim 30 wherein the additional data is data indicating a unique identification of the device.

45. A secure storage device comprising:
(a) means for receiving digital camera data from a digital camera;
(b) means for creating secure data from said digital camera data;
(c) means for storing data; and
(d) means for sending data to a destination.

46. An apparatus as recited in claim 45 wherein the secure storage device is responsive to the same protocol and file system structure as an unsecure device and as a result the secure device is transparent to the camera, whereby the camera responds to the secure device as if it were an unsecure storage device.

47. An apparatus as recited in claim 45 wherein the secure device is responsive to the same protocol and file system structure as an unsecure storage device and as a result the secure storage device is transparent to the destination, whereby the destination responds to the secure device as if it were an unsecure storage device.

48. An apparatus as recited in claim 45 further comprising means for inputting additional data to the secure storage device.

49. An apparatus as recited in claim 48 further comprising:
means for including the additional data with the secure data.

50. An apparatus as recited in claim 49 further comprising:
means for encrypting the additional data.

51. An apparatus as recited in claim 48 wherein the means for inputting includes means for inputting data from a computer.

52. An apparatus as recited in claim 45 wherein the means for creating includes means for receiving a security key for encrypting data.

53. An apparatus as recited in claim 45 further comprising a built in clock.

54. An apparatus as recited in claim 49 wherein the additional data includes absolute time and date.

55. An apparatus as recited in claim 49 wherein the means for inputting additional data includes means for inputting from a camera.

56. An apparatus as recited in claim 55 wherein the additional data includes a time and date of taking a picture.

57. An apparatus as recited in claim 49 further comprising a built in counter.

58. An apparatus as recited in claim 57 wherein the additional data includes a unique image identification number provided by the counter.

59. An apparatus as recited in claim 49 wherein the additional data is a unique identification of the device.

60. An apparatus as recited in claim 45 wherein the means for creating includes means for encrypting the digital camera data.

61. An apparatus as recited in claim 45 wherein the means for creating includes means for creating secure authentication data from the digital camera data.

62. An apparatus as recited in claim 49 wherein the secure data includes fingerprinted digital camera data, and the

fingerprinted digital camera data includes selected additional data.

63. An apparatus as recited in claim 45 wherein the camera is for taking still pictures.

64. An apparatus as recited in claim 45 wherein the camera is a video camera.

65. An apparatus as recited in claim 45 wherein the secure storage device has the external, physical configuration of a PCMCIA card.

66. An apparatus comprising:
(a) means for receiving digital camera data from a digital camera;
(b) means for creating secure data from the digital camera data; and
(c) means for sending the secure data to a destination.

67. An apparatus as recited in claim 66 further comprising a security device containing said means for creating.

68. An apparatus as recited in claim 67 wherein the means for receiving includes a cable assembly for connection from the security device to the digital camera.

69. An apparatus as recited in claim 68 wherein the security device further includes means for inputting additional data to the device.

70. An apparatus as recited in claim 69 wherein the means for inputting includes as PCMCIA card slot.

71. An apparatus as recited in claim 69 wherein the output means includes an output cable assembly for connecting from the security device to the destination.

72. An apparatus as recited in claim 69 wherein the output means includes

(a) first transceiver means for sending a radiated signal containing data from the security means; and

(b) second transceiver means for receiving the radiated signal for transmission to the destination.

73. An apparatus as recited in claim 71 wherein the camera is a still camera configured for taking still pictures.

74. An apparatus method as recited in claim 71 wherein the camera is a video camera.

75. An apparatus as recited in claim 69 further comprising means for securing the additional data.

76. An apparatus as recited in claim 69 wherein the means for inputting includes means for inputting the additional data from a computer.

77. An apparatus as recited in claim 69 further comprising means for inputting a security key to the security device.

78. An apparatus as recited in claim 69 wherein the security device includes a built-in clock.

79. An apparatus as recited in claim 78 wherein the additional data includes absolute time and date for setting the clock.

80. An apparatus as recited in claim 69 wherein the means for inputting includes means for inputting additional data to the device from a camera.

81. An apparatus as recited in claim 78 wherein the additional data includes a time and date of taking a picture.

82. An apparatus as recited in claim 69 wherein the security device includes a built-in counter.

83. An apparatus as recited in a claim 82 wherein the security device further includes means for creating data indicating a unique image identification number based on the counter.

84. An apparatus as recited in claim 69 wherein the additional data includes a unique identification of the secure storage device.

85. An apparatus as recited in claim 69 wherein the secure data includes encrypted digital camera data.

86. An apparatus as recited in claim 69 wherein the secure data includes authentication data created from digital camera data.

87. An apparatus as recited in claim 69 wherein the secure data includes fingerprinted digital camera data, and the fingerprinted digital camera data includes selected additional data.

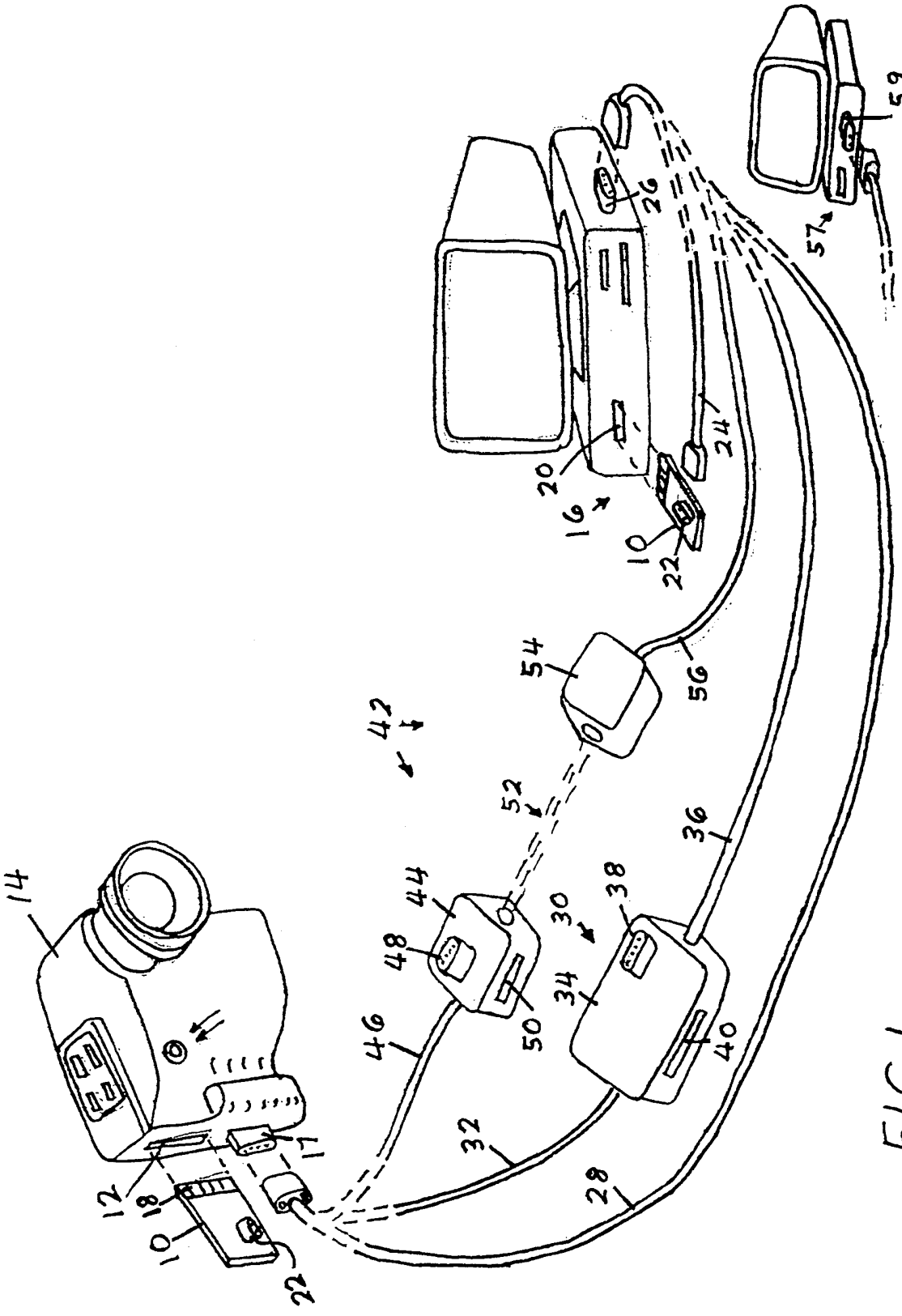

59
57
26
24
20
16
10
22
54
56
42
52
36
14
44
48
30
38
34
50
40
46
32
28
12
18
10
22

FIG 1

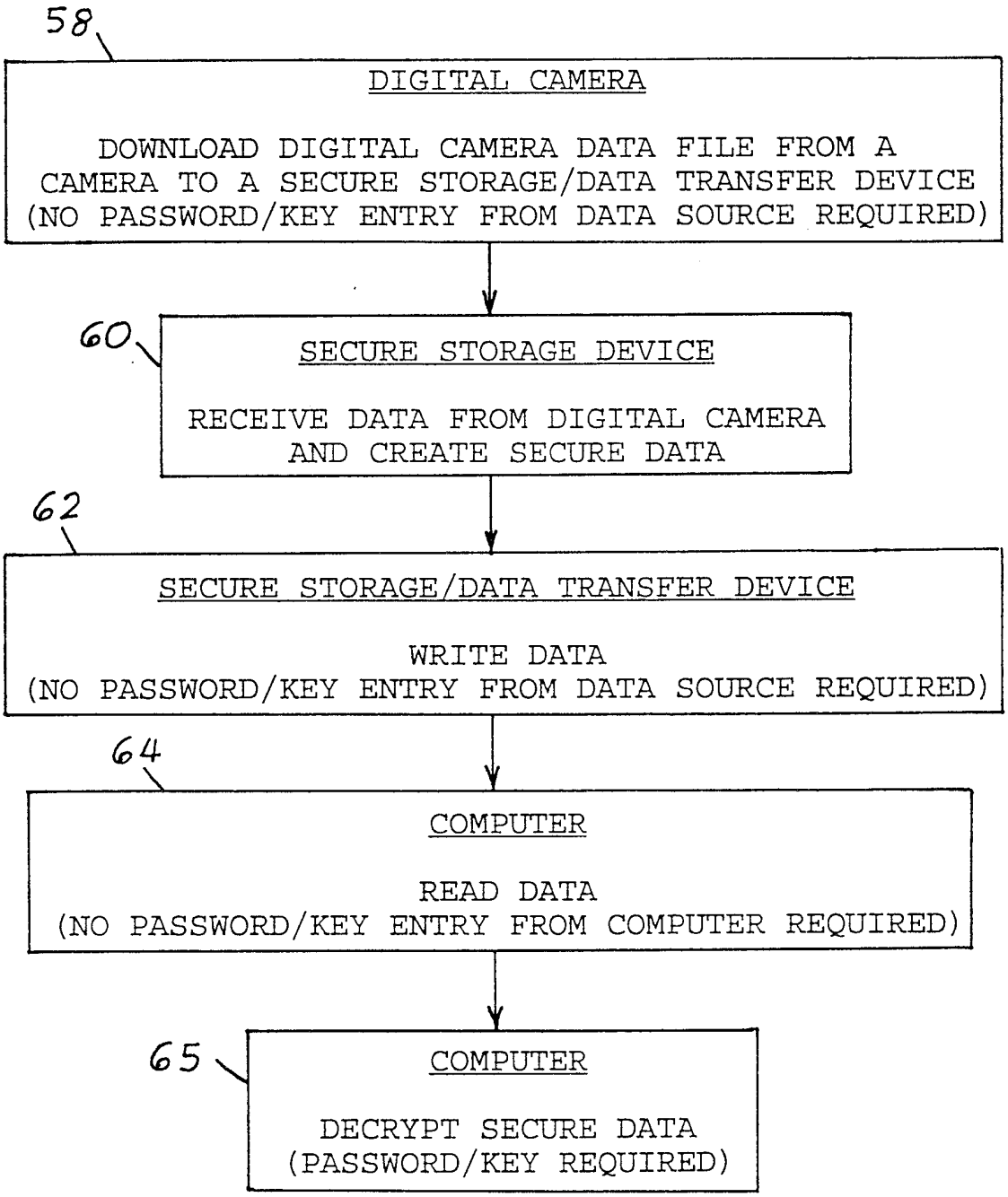

58
DIGITAL CAMERA
DOWNLOAD DIGITAL CAMERA DATA FILE FROM A CAMERA TO A SECURE STORAGE/DATA TRANSFER DEVICE (NO PASSWORD/KEY ENTRY FROM DATA SOURCE REQUIRED)
60
SECURE STORAGE DEVICE
RECEIVE DATA FROM DIGITAL CAMERA AND CREATE SECURE DATA
62
SECURE STORAGE/DATA TRANSFER DEVICE
WRITE DATA
(NO PASSWORD/KEY ENTRY FROM DATA SOURCE REQUIRED)
64
COMPUTER
READ DATA
(NO PASSWORD/KEY ENTRY FROM COMPUTER REQUIRED)
65
COMPUTER
DECRYPT SECURE DATA
(PASSWORD/KEY REQUIRED)

FIG 2

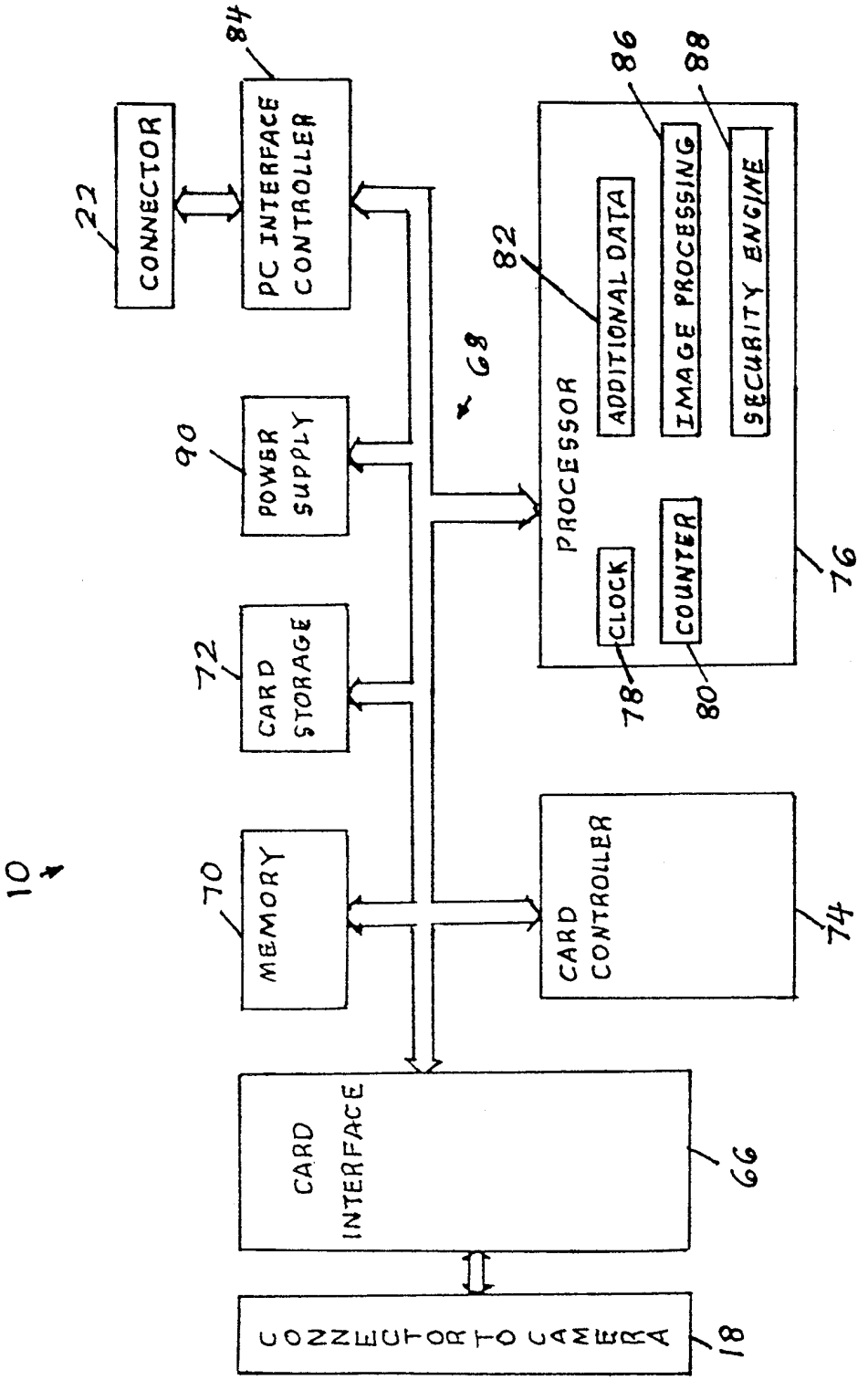

10
CONNECTOR
22
PC INTERFACE CONTROLLER
84
68
82
PROCESSOR
ADDITIONAL DATA
86
IMAGE PROCESSING
88
SECURITY ENGINE
76
CLOCK
78
COUNTER
80
POWER SUPPLY
90
CARD STORAGE
72
MEMORY
70
CARD CONTROLLER
74
CARD INTERFACE
66
CONNECTOR TO CAMERA
18

FIG 3

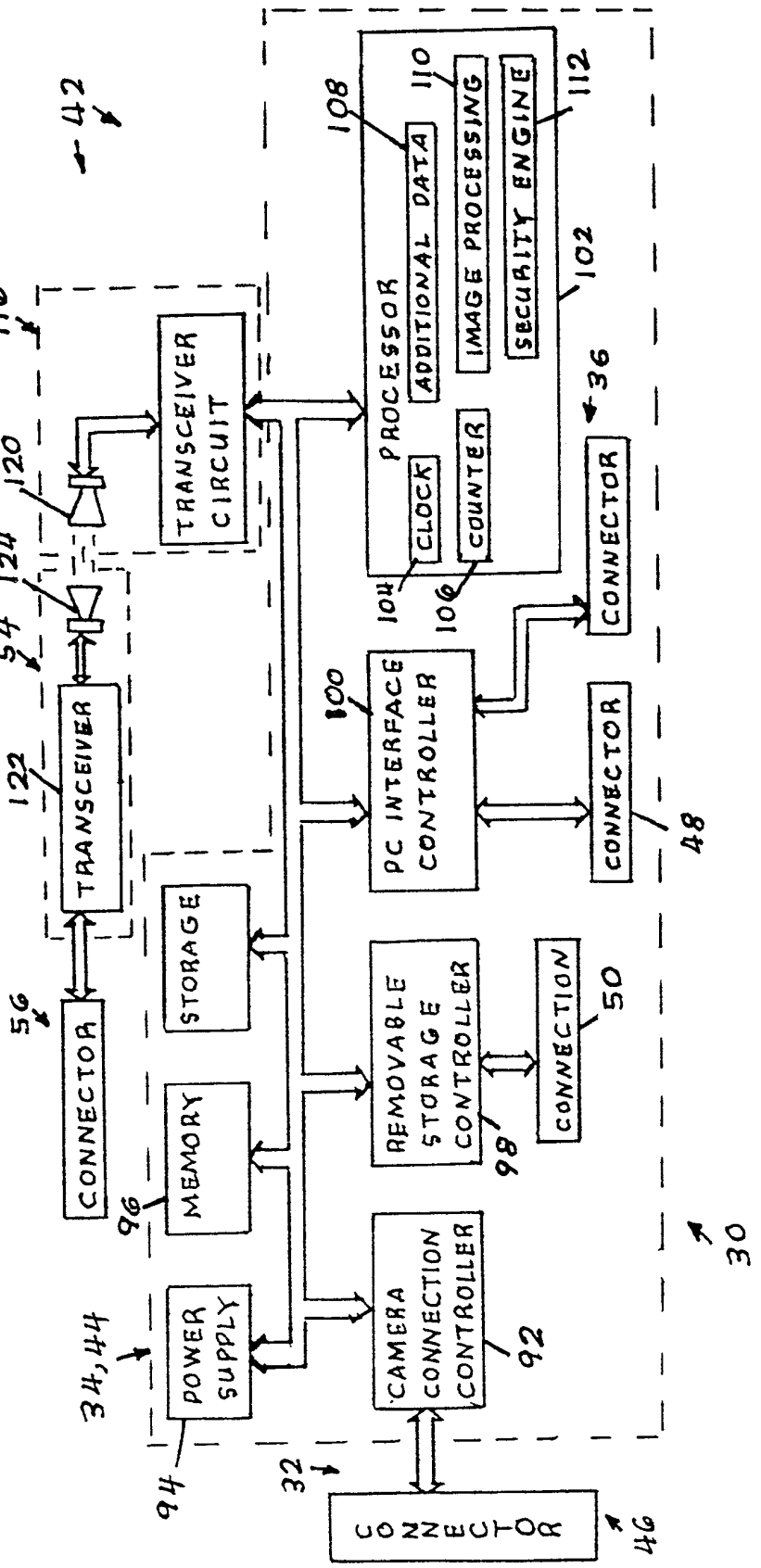

42
116
120
124
54
122
56
TRANSCEIVER CIRCUIT
TRANSCEIVER
CONNECTOR
STORAGE
MEMORY
POWER SUPPLY
34, 44
46
32
CAMERA CONNECTION CONTROLLER
92
REMOVABLE STORAGE CONTROLLER
98
CONNECTION
50
PC INTERFACE CONTROLLER
100
96
94
CONNECTOR
48
CONNECTOR
36
PROCESSOR
102
CLOCK
104
COUNTER
106
ADDITIONAL DATA
108
IMAGE PROCESSING
110
SECURITY ENGINE
112
30

FIG 4

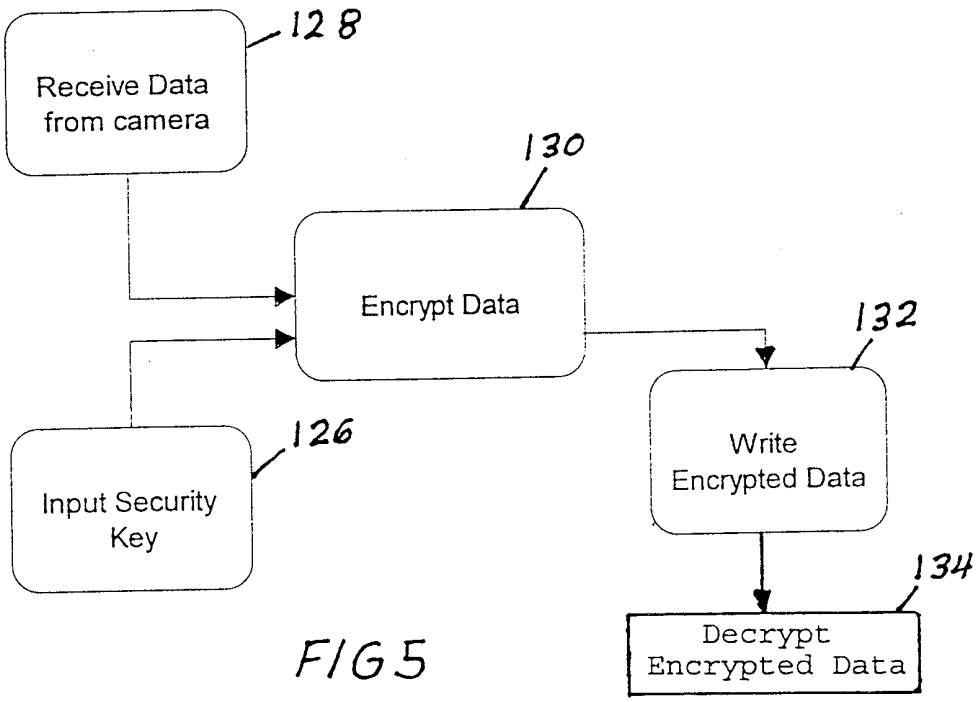

128
Receive Data from camera
130
Encrypt Data
132
Write Encrypted Data
126
Input Security Key
134
Decrypt Encrypted Data

FIG 5

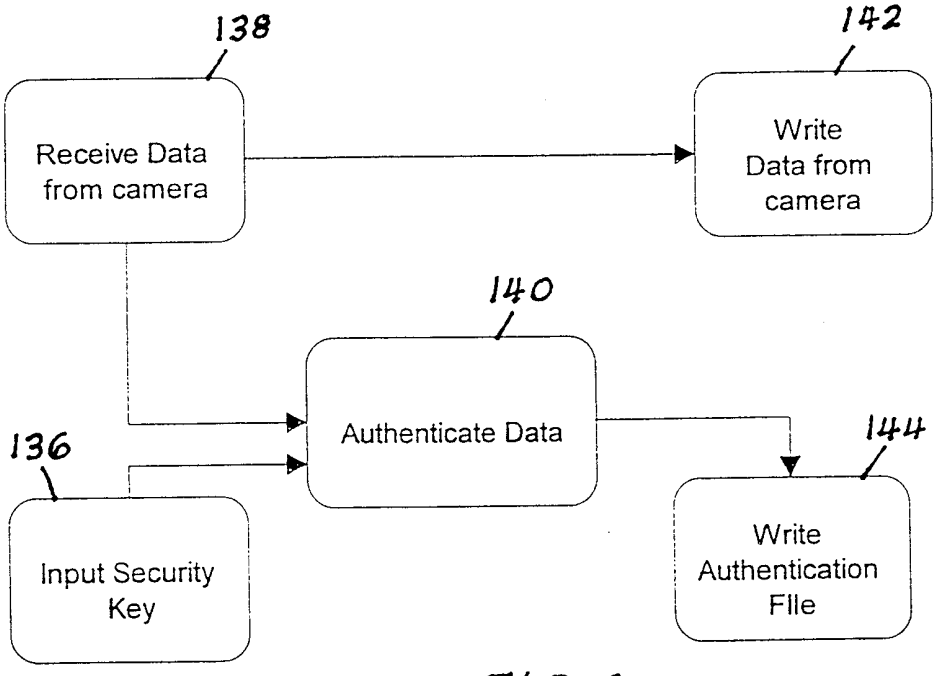

138
Receive Data from camera
142
Write Data from camera
140
Authenticate Data
136
Input Security Key
144
Write Authentication File

FIG 6

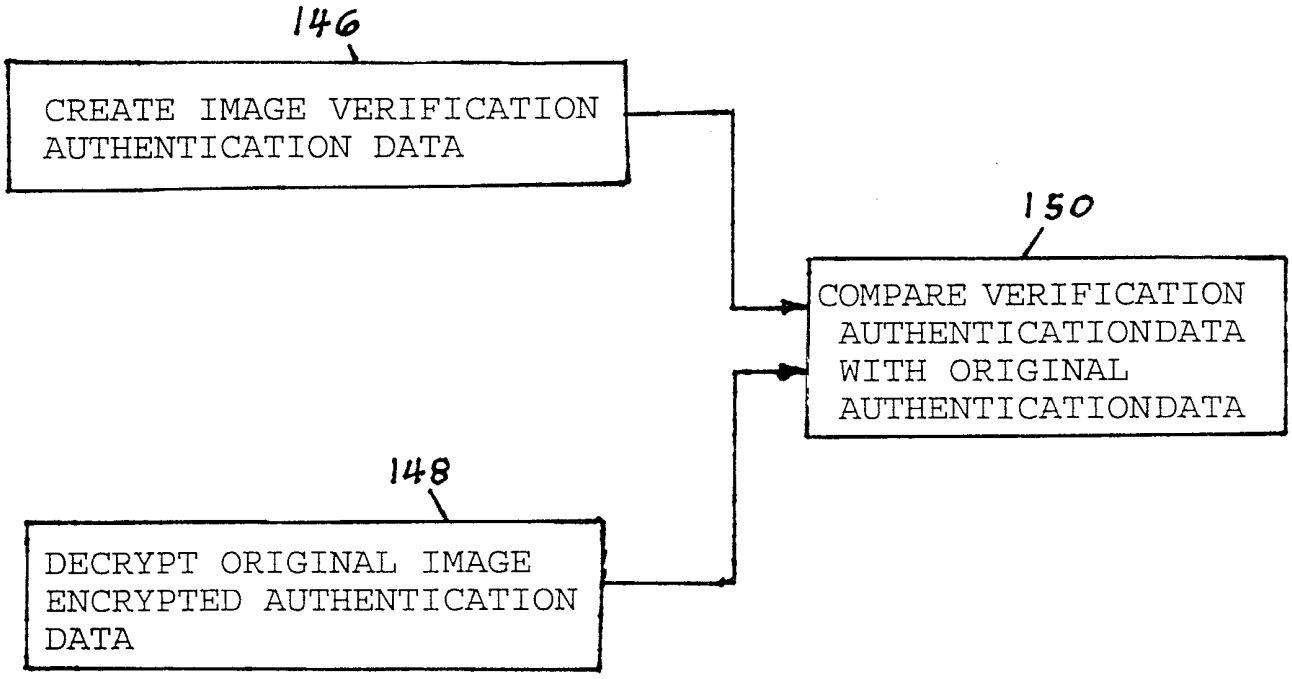

146
CREATE IMAGE VERIFICATION AUTHENTICATION DATA
150
COMPARE VERIFICATION AUTHENTICATIONDATA WITH ORIGINAL AUTHENTICATIONDATA
148
DECRYPT ORIGINAL IMAGE ENCRYPTED AUTHENTICATION DATA

FIG 7

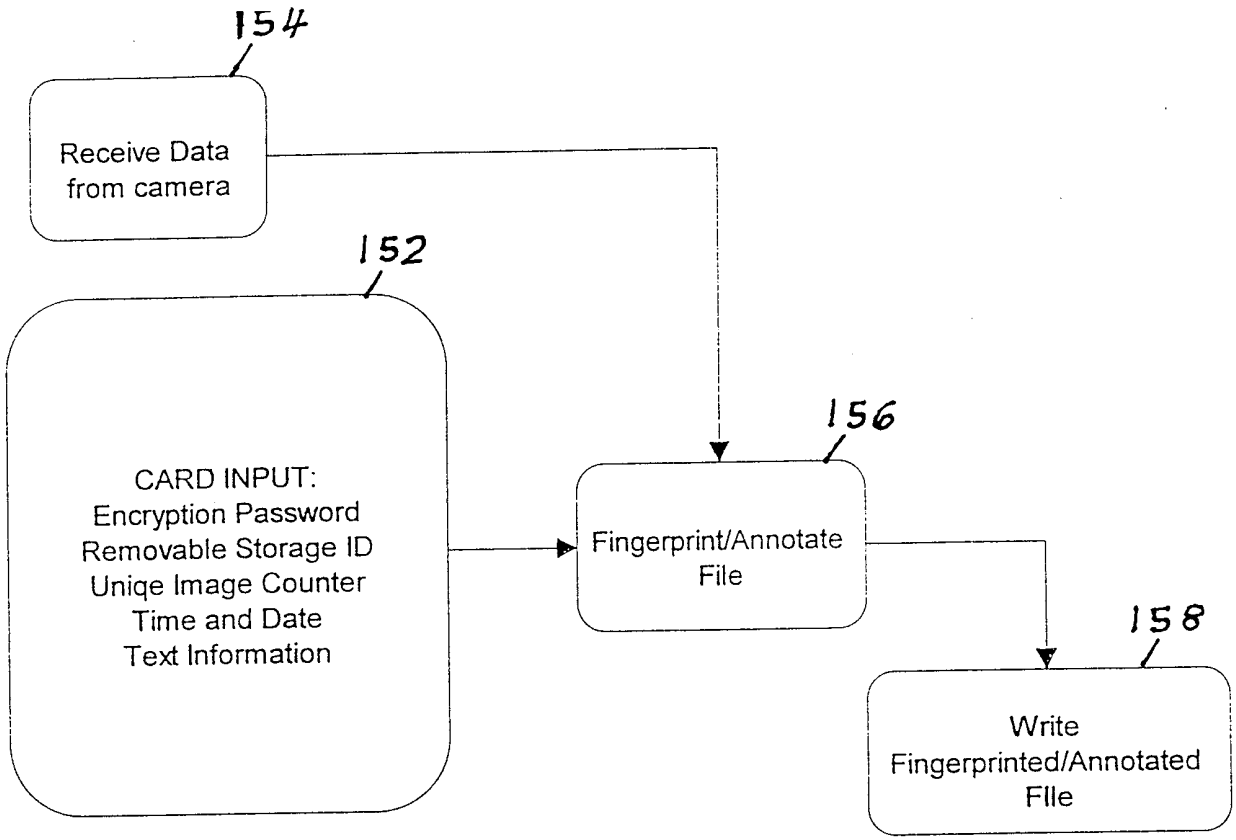

154
Receive Data from camera
152
CARD INPUT:
Encryption Password
Removable Storage ID
Uniqe Image Counter
Time and Date
Text Information
156
Fingerprint/Annotate File
158
Write Fingerprinted/Annotated FIle

FIG 8

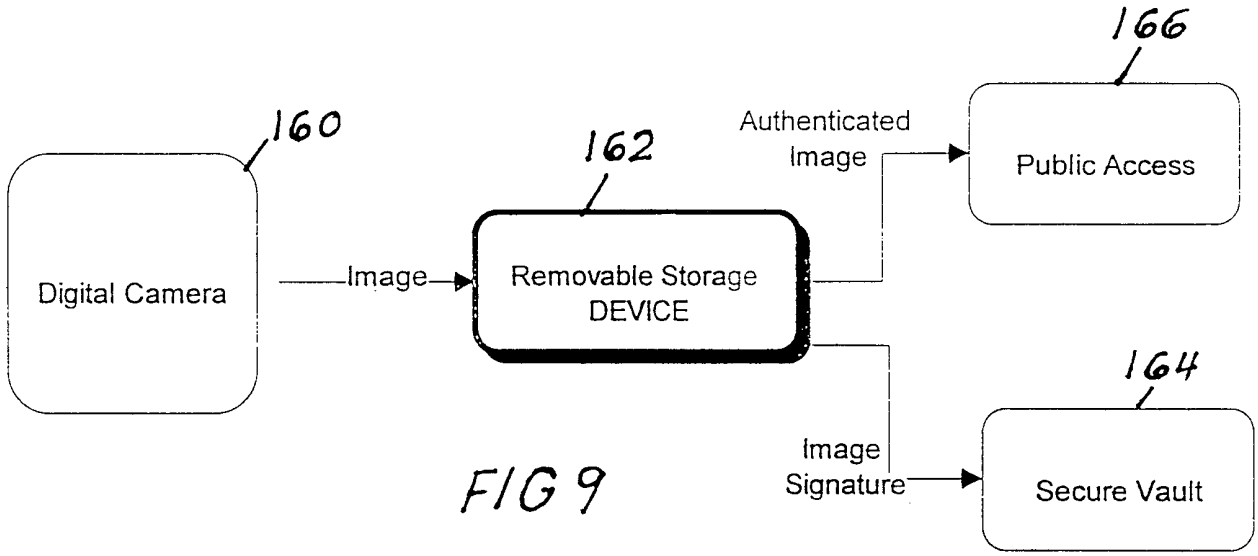

166
Public Access
Authenticated Image
160
Digital Camera
Image
162
Removable Storage DEVICE
164
Image Signature
Secure Vault

FIG 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/10390

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G06F 12/14
US CL :713/200
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200; 380/23

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS
search terms: digital camera, encryption, storage, media, secure storage

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,751,809 A (DAVIS et al.) 12 May 1998, column 7, lines 47-67, column 8, lines 1-50, column 9, lines 5-40.	1-87
X	US 5,027,401 A (SOLTESZ) 25 June 1991, column 7, lines 55-68, column 8, lines 1-55.	1, 2, 11, 21, 28, 37, 45-47, 60, 63, 66
Y,P	US 5,898,779 A (SQUILLA et al.) 27 April 1999, Figure 2	1-87
Y	US 5,666,516 A (COMBS) 09 September 1997 Figure 1A-1, Figure 1A-2.	1-87
A	US 5,677,953 A (DOLPHIN) 14 October 1997, Figure 1 and 2	1-87

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

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
17 AUGUST 1999	13 SEP 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Pinchus Laufer Telephone No. (703) 306-5538

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