

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
25 June 2009 (25.06.2009)

PCT

(10) International Publication Number
WO 2009/078554 A1

(51) International Patent Classification:
H04N 5/265 (2006.01)

(21) International Application Number:
PCT/KR2008/005399

(22) International Filing Date:
11 September 2008 (11.09.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2007-0132817
17 December 2007 (17.12.2007) KR

(71) Applicant (for all designated States except US): **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE** [KR/KR]; 161, Gajeong-dong, Yuseong-gu, Daejeon 305-350 (KR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **LEE, Deok Gyu** [KR/KR]; 315-10, Haegok-dong, Yongin-si, Kyunggi-do 449-090 (KR). **LEE, Yun Kyung** [KR/KR]; 114-702 Han-maeul Apt., Songgang-dong, Yuseong-gu, Daejeon 305-756 (KR). **KIM, Geon Woo** [KR/KR]; 201-1402

Yeolmae-maeul, Jjok-dong, Yuseong-gu, Daejeon 305-769 (KR). **HAN, Jong Wook** [KR/KR]; 1104-601 Yeolmae-maeul, 11Danji, Noeun-dong, Yuseong-gu, Daejeon 305-768 (KR). **CHUNG, Kyo Il** [KR/KR]; 107-1102 Hanul Apt., Sinseong-dong, Yuseong-gu, Daejeon 305-707 (KR). **JANG, Jong Soo** [KR/KR]; 303-903 Expo Apt., Jeonmin-dong, Yuseong-gu, Daejeon 305-761 (KR).

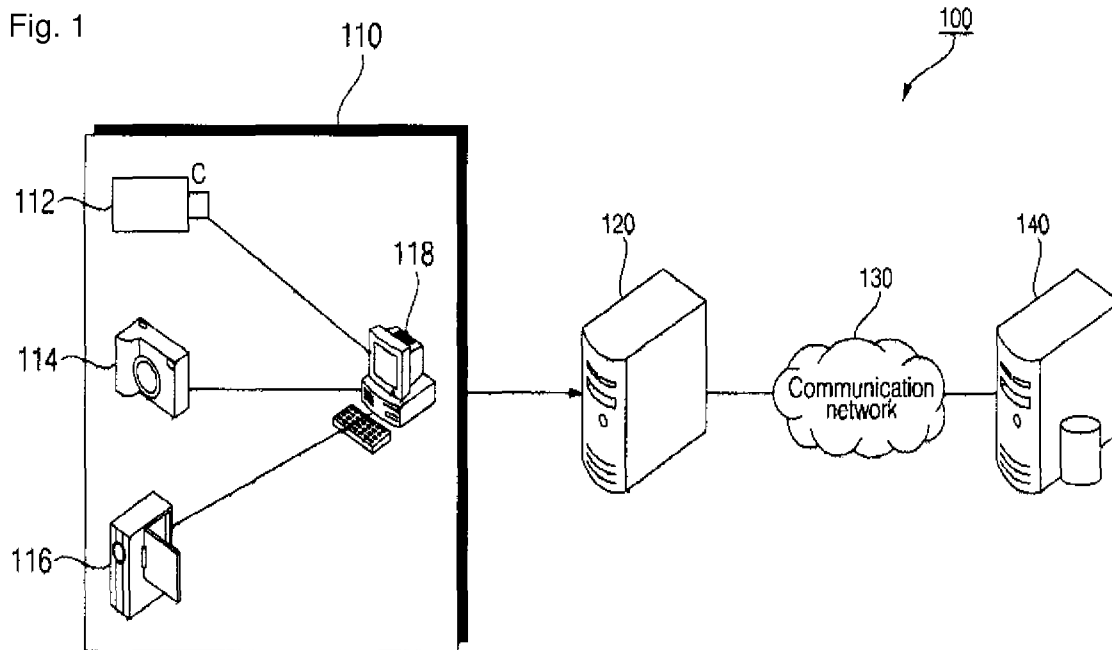
(74) Agent: **PARK, Byung Chang**; 2F Dongju Bldg., 824-24 Yeoksam-dong, Kangnam-gu, Seoul 135-080 (KR).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: APPARATUS AND METHOD FOR PROCESSING IMAGE INFORMATION



(57) Abstract: An apparatus and a method for processing image information are provided. The apparatus for processing image information includes an image capturing device and an image information server for receiving and storing an image captured by the image capturing device and adds information on the image capturing device and signature information to image data obtained by the image capturing device. Accordingly, the device information and the signature information can be added to the image data obtained by the image capturing device to maintain security of the image data and use the image data as digital proof when a specific event is generated.

WO 2009/078554 A1



ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL,
NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG,
CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

Description

APPARATUS AND METHOD FOR PROCESSING IMAGE INFORMATION

Technical Field

- [1] The present invention relates to an apparatus and a method for processing image information, and more particularly, to an image information processing apparatus and method capable of adding information on an image capturing device and signature information to image data and storing the image data to maintain security of the image data and use the image data as digital proof.
- [2] The present invention was supported by the IT R&D program of Ministry of Information and Communication(MIC) and Institute for Information Technology Advancement(IITA)[Project No.: 2006-S-067-02, Project Title: Development of ubiquitous home network security technology based on device authentication].

[3]

Background Art

- [4] With the development of image photographing technology, techniques for maintaining security of image data captured by an image capturing device and protecting copyright are proposed. For example, captured images are transmitted to a limited image information output device and reproduced or identification information such as watermarking is embedded in image data to protect copyright of image information.
- [5] In the case of embedding watermarking in image information, it is possible to confirm the copyright holder of the image information even though the image information is displayed at or transmitted to an undesired place and prevent the image information from being illegally copied. Furthermore, users can watch the image information without having any difficulty and track the source of the image information and image information copy routes when watermarking is embedded in the image information.
- [6] However, watermarking does not have legal force capable of preventing the image information from being illegally copied or transmitted although it can show the copyright holder or the source of the image information and allow users to confirm image information copy routes and the source of the image information. Accordingly, security of image information cannot be efficiently maintained only with watermarking when the image information includes personal information related to privacy or data requiring the maintenance of security.

[7]

Disclosure of Invention

Technical Problem

- [8] It is an object of the present invention to provide an image information processing apparatus and method for adding information on an image capturing device and predetermined signature information to image data obtained using the image capturing device to protect the image data from infringement of security such as illegal copy and transmission and adding information on the place and time at which the image data is obtained to the image data to use the image data as digital proof.

[9]

Technical Solution

- [10] An apparatus for processing image information according to the present invention comprises: an image capturing unit for generating image data and collecting information on the image capturing unit; an image processing unit for adding at least one of the information on the image capturing unit and signature information to the image data using the image data and the information on the image capturing unit transmitted from the image capturing unit; and an image storage unit for storing the image data output from the image processing unit.
- [11] A method for processing image information according to the present invention comprises: an image capturing step of generating image data and collecting information on the image capturing step; an image processing step of adding at least one of the information on the image capturing step and signature information to the image data; and an image storing step of storing the image data.
- [12]
- [13] An apparatus for processing image information using image data according to the present invention comprises: a device information unit for embedding information on the device that generates the image data in the image data; a signature information unit for embedding signature information in the image data; and a storage unit for storing the image data having at least one of the information on the device and the signature information added thereto.
- [14] A method for processing image information using image data according to the present invention comprises: a device information step of embedding information on the device that generates the image data in the image data; a signature information step of embedding signature information in the image data; and a storing step of storing the image data having at least one of the information on the device and the signature information added thereto.
- [15]

Advantageous Effects

- [16] The present invention can acquire image data included in a captured image and add information on the device that captures the image and signature information to the image data to efficiently maintain security of the image data and use a captured image with respect to a specific event as digital proof.

[17]

Brief Description of the Drawings

- [18] The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this application, illustrate embodiment(s) of the invention and together with the description serve to explain the principle of the invention. In the drawings:
- [19] FIG. 1 is a view illustrating a configuration of an image photographing system to which an image information processing apparatus according to the present invention is applied;
- [20] FIG. 2 is a block diagram of an image capturing device 110 and an image information server 120 illustrated in FIG. 1 according to an embodiment of the present invention;
- [21] FIG. 3 is a block diagram of an image capturing device 110 and an image information server 120 illustrated in FIG. 1 according to another embodiment of the present invention; and
- [22] FIG. 4 is a flow chart of an image information processing method using the image photographing system illustrated in FIG. 1.

[23]

Best Mode for Carrying Out the Invention

- [24] Hereinafter, an embodiment of the present invention will be described below with reference to the accompanying drawings.
- [25] FIG. 1 is a view illustrating a configuration of an image photographing system to which an image information processing apparatus according to the present invention is applied. Referring to FIG. 1, the image photographing system includes an image capturing device 110 for capturing an image and converting the captured image into image data, an image information server 120 for receiving and storing the image data, and an application server 140 for providing various application services using the image data stored in the image information server 120.
- [26] The image capturing device 110 includes an imaging capturing unit 112 for converting an optical image formed through a lens into image data and an image processor 118 for receiving the image data and adding signature information or device information of the image capturing unit 112 to the image data.
- [27] The image capturing unit 112 that is a device capable of capturing an image can be a

closed-circuit television (CCTV), a digital camera or a video camera, for example. The image capturing unit 112 includes a lens for condensing light and a charge-coupled device (CCD) for converting the light condensed by the lens into image data, recognizes an object through the lens and images the recognized object to generate an optical image. This optical image can be converted into image data through a CCD sensor. The image data generated by the image capturing unit 112 is transmitted to the image processor 118.

- [28] The image processor 118 receives the image data from the image capturing unit 112, processes the image data and embeds signature information in the image data. The image processor 118 can be constructed as additional hardware or included in the image capturing unit 112. In the current embodiment, it is assumed that the image processor 118 exists as an additional module separated from the image capturing unit 112.
- [29] The image processor 118 adds at least one of information on the image capturing unit 112 and signature information to the image data transmitted from the image capturing unit 112. By doing so, the image data can be protected from arbitrary access and control. The signature information can be added to the image data at regular intervals.
- [30] The image information server 120 stores the image data to which the information on the image capturing unit 112 or the signature information has been added by the image processor 118. The image information server 120 includes a storage unit capable of storing the image data having the information on the image capturing unit 112 or the signature information added thereto and can be connected to a communication network 130 such as the Internet or a mobile communication network to transmit the image data processed by the image processor 118 to a communication terminal. That is, the image data processed by the image processor 118 can be stored in the image information server 120 and applied to the application server 140 through the communication network 130 such as the Internet.
- [31] The application server 140 provides a variety of application services to a mobile terminal of a communication service subscriber using the communication network 130 at the request of the communication service subscriber. For example, the application server 140 extracts the stored image data and transmits the image data to a mobile terminal at the request of the user of the mobile terminal. The application server 140 can store the image data to which information such as signature information has been added by the image processor 118 or the image information server 120 and transmit the stored image data to the terminal of the communication service substrate to prevent the image data from being illegally copied and edited.
- [32] In another embodiment, the image information server 120 can add the signature information or the information on the image capturing unit 112 to the image data

captured by the image capturing unit 112. In this case, the image processor 118 transmits the image data and the information on the image capturing unit 112 received from the image capturing unit 112 to the image information server 120, and the image information server 120 adds the information on the image capturing unit 112 or the signature information to the image data transmitted from the image processor 118. The image data processed by the image information server 120 can be applied to the application server 140 through the communication network 130 such as the Internet. This will be explained in more detail later with reference to FIG. 3.

- [33] FIG. 2 is a block diagram of the image capturing device 110 and the image information server 120 illustrated in FIG. 1 according to an embodiment of the present invention, which shows a case in which the image processor 118 adds the information on the image capturing unit 112 or the signature information to the image data.
- [34] Referring to FIG. 2, the image photographing device 110 includes the image capturing unit 112 and the image processor 118. The image processor 118 includes an information receiver 232, a device information processor 234, a signature information processor 236, and an image transmitter 238. The image information server 120 includes an image receiver 242 and a storage unit 244.
- [35] The image capturing unit 112 is a device capable of capturing an image, obtaining image data from the captured image and collecting information on the image capturing unit 112. For example, a CCTV, a digital camera, a video camera or a communication terminal including a camera module can be used as the image capturing unit 112. The image data obtained by the image capturing unit 112 is transmitted to the image processor 118 and undergoes a data processing operation of adding signature information or the information on the image capturing unit 112 thereto.
- [36] The image processor 118 adds the information on the image capturing unit 112 or the signature information to the image data generated by the image capturing unit 112. The information receiver 232 included in the image processor 118 receives the image data generated by the image capturing unit 112 and the information on the image capturing unit 112 and the device information processor 234 adds the information on the image capturing unit 112 to the image data transmitted from the information receiver 232. The signature information processor 236 adds the signature information to the image data transmitted from the device information processor 234 and the image transmitter 238 transmits the image data having the information on the image capturing unit 112 or the signature information added thereto to the image information server 120.
- [37] Here, positions of the device information processor 234 and the signature information processor 236 can be changed each other. That is, the signature information can be added first, and then the information on the image capturing unit can be added.
- [38] The information receiver 232 receives the image data generated by the image

capturing unit 112 and transmits the information to the device information processor 234. The information on the image capturing unit 112 can include an identifier given to the image capturing unit 112 or information on the place and time at which the image capturing unit 112 obtains the image data. When the image capturing unit 112 is a CCTV, for example, the information on the image capturing unit 112 can include the place where the CCTV is installed and the time when the CCTV records the image. When the image capturing unit 112 is a communication terminal, the information on the image capturing unit 112 can include an identification number given to the communication terminal.

- [39] The device information processor 234 adds the information on the image capturing unit 112 to the image data transmitted from the information receiver 232. That is, the place and time at which the image data is obtained or the identification number of the image capturing unit 112 that captures the image data can be added to the image data as the information on the image capturing unit 112. The image data can be used as digital proof of a specific event when the place and time at which the image data is captured is added thereto and the source of the image data can be easily detected when the identification number of the image capturing unit 112 is added thereto. The device information processor 234 transmits the image data having the information on the image capturing unit 112 added thereto to the signature information processor 236.
- [40] The signature information processor 236 can embed signature information including a predetermined encryption key in the image data transmitted from the device information processor 234. According to an embodiment, the signature information processor 236 can add public key based signature information, symmetric key based signature information or public key and symmetric key based signature information to the image data.
- [41] The public key based signature information can be generated according to Rivest Shamir Adleman (RSA) algorithm and the symmetric key based signature information can be generated according to Vernam or data encryption standard (DES) algorithm. The symmetric key based signature information requires transmission of an additional secret key and is difficult to authenticate with safety although it is encrypted at a high speed. On the other hand, the public key based signature information does not require transmission of the additional secret key and is easily authenticated with safety while it is encrypted at a low speed. Accordingly, an algorithm of generating the signature information can be selected according to a degree to which maintenance of security of the image data is required.
- [42] When the signature information is added to the image data, the image data can be accessed only using a predetermined decryption key. Accordingly, the possibility that the image data is exposed to hacking or illegal copy according to arbitrary access can

be reduced when the signature information is added to the image data. The application server 140 that provides the image data to communication subscribers can provide the decryption key to only an authenticated communication subscriber through a text message to maintain security of the image data.

[43] The signature information can be added to the image data at regular intervals.

[44] The image data having the information on the image capturing unit 112 and the signature information added thereto is transmitted to the image transmitter 238. That is, at least one of the information on the image capturing unit 112 and the signature information is added to the image data transmitted from the image capturing unit 112 and transmitted to the image transmitter 238.

[45] The image transmitter 238 transmits the image data received from the signature information processor 236 to the image information server 120.

[46] The image receiver 242 receives the image data from the image transmitter 238. The storage unit 244 stores the image data transmitted from the image receiver 242. The image data transmitted from the image receiver 242 has at least one of the information on the image capturing unit 112 and the signature information added thereto.

[47] The image information server 120 can determine whether the decryption key transmitted from the application server 130 corresponds to the encryption key embedded in the image data, extract the image data stored in the storage unit 244 and transmit the image data to the application server 140 when the application server 140 requests the image information server 120 to transmit the image data through the communication network 130.

[48] FIG. 3 is a block diagram of the image capturing device 110 and the image information server 120 illustrated in FIG. 1 according to another embodiment of the present invention, which shows a case in which the image information server 120 adds the information on the image capturing unit 112 or the signature information to the image data.

[49] Referring to FIG. 3, the image capturing device 110 includes the image capturing unit 112 and the image processor 118 and the image information server 120 includes a receiver 322, a device information processor 324, a signal information processor 326 and a storage unit 328.

[50] The image capturing unit 112 is a device capable of recognizing an object through a lens and a sensor, obtaining image data from the recognized object and collecting information on the image capturing unit 112. The image processor 118 transmits the image data and the information on the image capturing unit 112 received from the image capturing unit 112 to the image information server 120.

[51] The receiver 322 included in the image information server 120 receives the image data and the information on the image capturing unit 112 transmitted from the image

processor 118 and the device information processor 324 receives the image data and the information on the image capturing unit 112 from the receiver 322 and embeds the information on the image capturing unit 112 in the image data. The signature information processor 326 adds predetermined signature information to the image data having the information on the image capturing unit 112 added thereto and the storage unit 328 stores the image data including the signature information.

[52] The receiver 322 receives the image data and the information on the image capturing unit 112 from the image processor 118.

[53] The device information processor 324 embeds the information on the image capturing unit 112 in the image data and transmits the image data to the signature information processor 326. The information on the image capturing unit 112 depends on the type of the image capturing unit 112. For example, when the image capturing unit 112 is a CCTV, the information on the image capturing unit 112 can include the place where the CCTV is installed and the time when the CCTV obtains the image data. When the image capturing unit 112 is a communication terminal including a camera module, the information on the image capturing unit 112 can include the identification number of the communication terminal.

[54] The source of the image data can be easily searched when the identification number of the image capturing unit 112 is embedded in the image data and the image data can be used as digital proof when the place and time at which the image capturing unit 112 captures the image data is added thereto. The information on the image capturing unit 112 can be recorded in a meta data region of the image data.

[55] The signature information processor 326 can embed signature information including a predetermined encryption key in the image data transmitted from the device information processor 324.

[56] The signature information processor 326 can generate the signature information according to a predetermined algorithm and embed the signature information in the image data. The signature information can be generated according to a public key based algorithm or a symmetric key based algorithm. In general, the case that the image information server 120 embeds the information on the image capturing unit 112 and the signature information in the image data requires a data processing speed and available capacity greater than the data processing speed and available capacity required for the case that the image photographing device 110 embeds the information on the image capturing unit 112 and the signature information in the image data. Accordingly, it is desirable to generate the signature information using the public key based algorithm that easily performs safe authentication and does not require an addition secret key to be transmitted while having a low encryption speed. The image data to which the signature information has been added is stored in the storage unit 328

of the image information server 120.

[57] The signature information can be added to the image data at regular intervals.

[58] The storage unit 328 stores the image data transmitted from the signature information processor 326. The image data transmitted from the signature information processor 326 has at least one of the information on the image capturing unit 112 and the signature information added thereto.

[59] The image information server 120 can receive a predetermined decryption key from the application server 140 and compare the decryption key with the encryption key included in the image data to determine whether the image data is transmitted when the application server 140 requests the image information server 120 to transmit the image data through the communication network 130.

[60] FIG. 4 is a flow chart of an image information processing method using the image photographing system illustrated in FIG. 1.

[61] Referring to FIG. 4, the image capturing unit 112 included in the image capturing device 110 recognizes an image and captures the image in operation S400.

[62] Then, the image capturing unit 112 acquires image data from the image captured in operation S400. For example, the image capturing unit 112 included in the image capturing device 110 can condense light through a lens and convert the light that has passed through the lens into image data using a CCD sensor.

[63] The image data can include meta data and main data. The main data can include information on the captured image and the meta data can include information that explains the main data.

[64] When the image data is obtained, the image capturing device 110 determines whether it is required to protect the image data in operation S420. It can be determined whether the image data requires protection according to the type of the image capturing device 110 or setting up by a user who captures the image.

[65] When it is determined that the image data does not require protection in operation S420, the image data is transmitted to the image information server 120 without undergoing additional image data processing in operation S480.

[66] When it is determined that the image data requires protection in operation S420, information on the image capturing device 100 is added to the image data in operation S430. For example, the information on the image capturing device 110 can correspond to information on the image capturing unit 112 that captures the image data and be added to the image data by the image processor 118 of the image capturing device 110 or the image information server 120. That is, when the image processor 118 is configured in the form of a module independent from the image capturing unit 112 or has sufficient data processing speed and capacity, the image processor 118 can add the information on the image capturing device 110 to the image data. However, when the

image processor 118 do not have sufficient data processing speed and capacity or is configured in the form of software installed in the image capturing unit 112, the image information server 120 can add the information on the image capturing device 110 to the image data.

- [67] When the information on the image capturing device 110 is embedded in the image data in operation S430, the type of signature information to be added to the image data is determined in operation S440. The signature information can be generated according to symmetric key based algorithm, public key based algorithm or public key and symmetric key based algorithm and embedded in the image data.
- [68] When the signature information according to the symmetric key based algorithm is embedded in the image data in operation S450, safe authentication is difficult to perform and an additional secret key is required although encryption speed is high due to low algorithm complexity. Accordingly, it is desirable to use the symmetric key based algorithm in consideration of data processing load applied to the image processor 118 in the case where the image processor 118 embeds the signature information in the image data.
- [69] When the signature information according to the public key based algorithm is embedded in the image data in operation S460, safe authentication can be achieved and transmission of an additional secret key is not needed in spite of high algorithm complexity. Accordingly, it is desirable to use the public key based algorithm using the data processing speed and capacity of the image information server 120, which are greater than those of the image processor 118 when the image information server 120 embeds the signature information in the image data.
- [70] When the signature information according to the public key and symmetric key mixed algorithm is embedded in operation S470, a public key is generated using the public key based algorithm first, and then a data encryption key with respect to the public key based algorithm is generated using the symmetric key based algorithm. Although the public key and symmetric key mixed algorithm can secure safe authentication as compared to the cases where the public key based algorithm and symmetric key based algorithm are used in operations S450 and S460, it is desirable to use the mixed algorithm when the image information server 120 can embed the signature information in the image data because algorithm complexity is high.
- [71] The signature information can be added to the image data at regular intervals.
- [72] When the signature information has been embedded in the image data in operations S450, S460 and S470, the image data having the signature information added thereto is stored in the image information server 120 in operation S480. When the application server 140 requests the image information server 120 to transmit the image data through the communication network 130, the image information server 120 can

compare the decryption key transmitted from the application server 140 with the encryption key included in the image data stored in the image information server 120 to determine whether the requested image data is transmitted.

[73] While the present invention has been particularly shown and described with reference to exemplary embodiments thereof, it will be understood by those of ordinary skill in the art that various changes in form and details may be made therein without departing from the spirit and scope of the present invention as defined by the following claims.

[74]

Industrial Applicability

[75] According to the present invention, image data can be protected from security infringement such as illegal copy and arbitrary transmission. Furthermore, information on the place and time at which an image is captured is added to the image data such that the image data can be used as digital proof.

[76]

[77]

Claims

- [1] An apparatus for processing image information comprising:
an image capturing unit for generating image data and collecting information on the image capturing unit;
an image processing unit for adding at least one of the information on the image capturing unit and signature information to the image data using the image data and the information on the image capturing unit transmitted from the image capturing unit; and
an image storage unit for storing the image data output from the image processing unit.
- [2] The apparatus of claim 1, wherein the image processing unit comprises:
a device information processor for embedding the information on the image capturing unit in the image data; and
a signature information processor for embedding the signature information in the image data.
- [3] The apparatus of claim 2, wherein the signature information processor adds the signature information to the image data using at least one of a public key base algorithm and a symmetric key based algorithm.
- [4] The apparatus of claim 1, wherein the information on the image capturing unit corresponds to information on the place and time at which the image capturing unit obtains the image data.
- [5] The apparatus of claim 1, wherein the signature information is added to the image data at regular intervals.
- [6] The apparatus of claim 1, further comprising an image authentication unit for comparing the signature information with a decryption key and determining whether the image data output from the image processing unit is transmitted when the image data is requested to be transmitted and the decryption key is transmitted thereto.
- [7] A method for processing image information comprising:
an image capturing step of generating image data and collecting information on the image capturing step;
an image processing step of adding at least one of the information on the image capturing step and signature information to the image data; and
an image storing step of storing the image data.
- [8] The method of claim 7, wherein the image processing step comprises:
a device information processing step of embedding the information on the image capturing step in the image data; and

a signature information processing step of embedding the signature information in the image data.

- [9] The method of claim 8, wherein the signature information processing step adds the signature information to the image data using at least one of a public key base algorithm and a symmetric key based algorithm.
- [10] The method of claim 7, wherein the information on the image capturing step corresponds to information on the place and time at which the image data is obtained.
- [11] The method of claim 7, wherein the signature information is added to the image data at regular intervals.
- [12] The method of claim 7, further comprising an image authentication step of comparing the signature information with a decryption key and determining whether the image data output from the image processing step is transmitted when the image data is requested to be transmitted and the decryption key is transmitted.
- [13] An apparatus for processing image information using image data, comprising:
 - a device information unit for embedding information on the device that generates the image data in the image data;
 - a signature information unit for embedding signature information in the image data; and
 - a storage unit for storing the image data having at least one of the information on the device and the signature information added thereto.
- [14] The apparatus of claim 13, wherein the information on the device corresponds to information on the place and time at which the image data is obtained.
- [15] The apparatus of claim 13, wherein the signature information unit adds the signature information to the image data using at least one of a public key base algorithm and a symmetric key based algorithm.
- [16] The apparatus of claim 13, wherein the signature information is added to the image data at regular intervals.
- [17] The apparatus of claim 13, further comprising an image authentication unit for comparing the signature information with a decryption key and determining whether the image data stored in the storage unit is transmitted when the image data is requested to be transmitted and the decryption key is transmitted thereto.
- [18] A method for processing image information using image data, comprising:
 - a device information step of embedding information on the device that generates the image data in the image data;
 - a signature information step of embedding signature information in the image data; and

a storing step of storing the image data having at least one of the information on the device and the signature information added thereto.

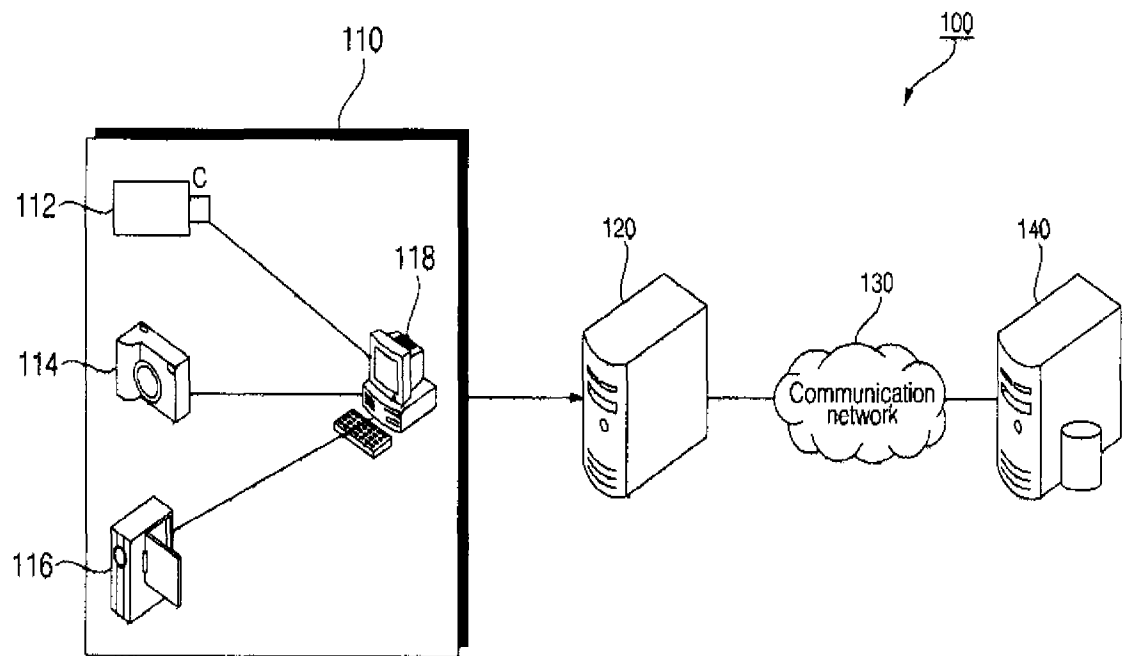
[19] The method of claim 18, wherein the information on the device corresponds to information on the place and time at which the image data is obtained.

[20] The method of claim 18, wherein the signature information step adds the signature information to the image data using at least one of a public key base algorithm and a symmetric key based algorithm.

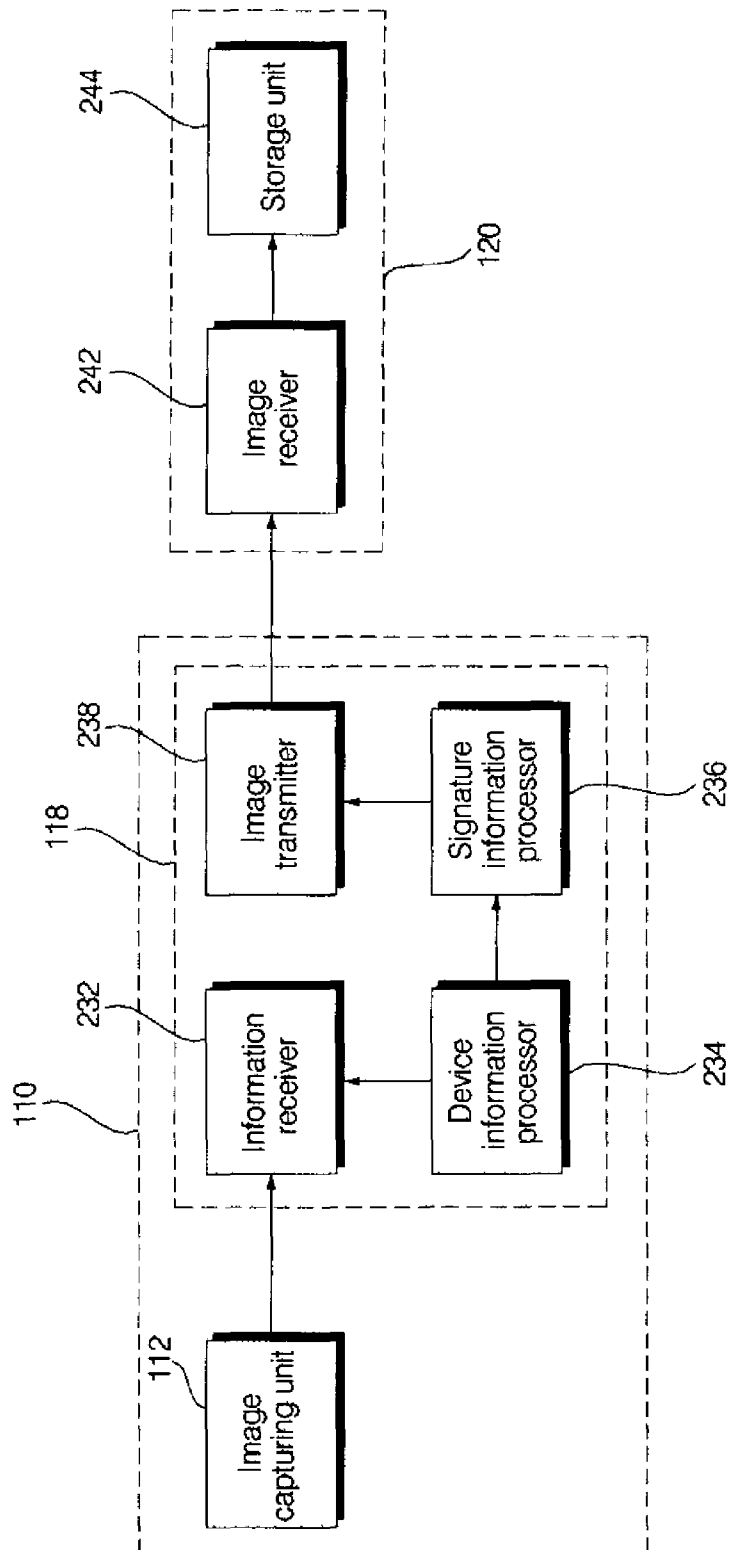
[21] The method of claim 18, wherein the signature information is added to the image data at regular intervals.

[22] The method of claim 18, further comprising an image authentication step of comparing the signature information with a decryption key and determining whether the image data stored in the storing step is transmitted when the image data is requested to be transmitted and the decryption key is transmitted.

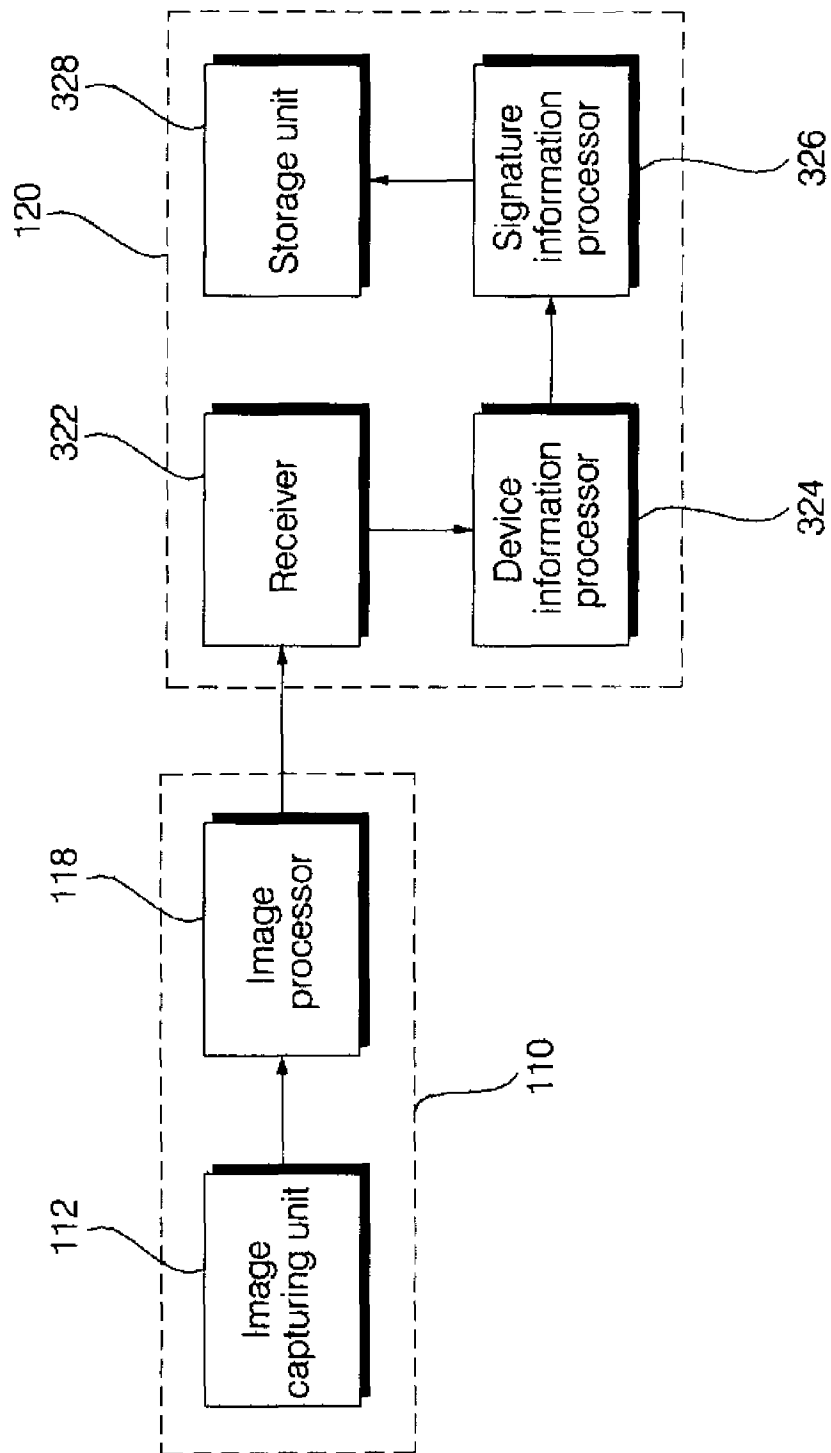
[Fig. 1]



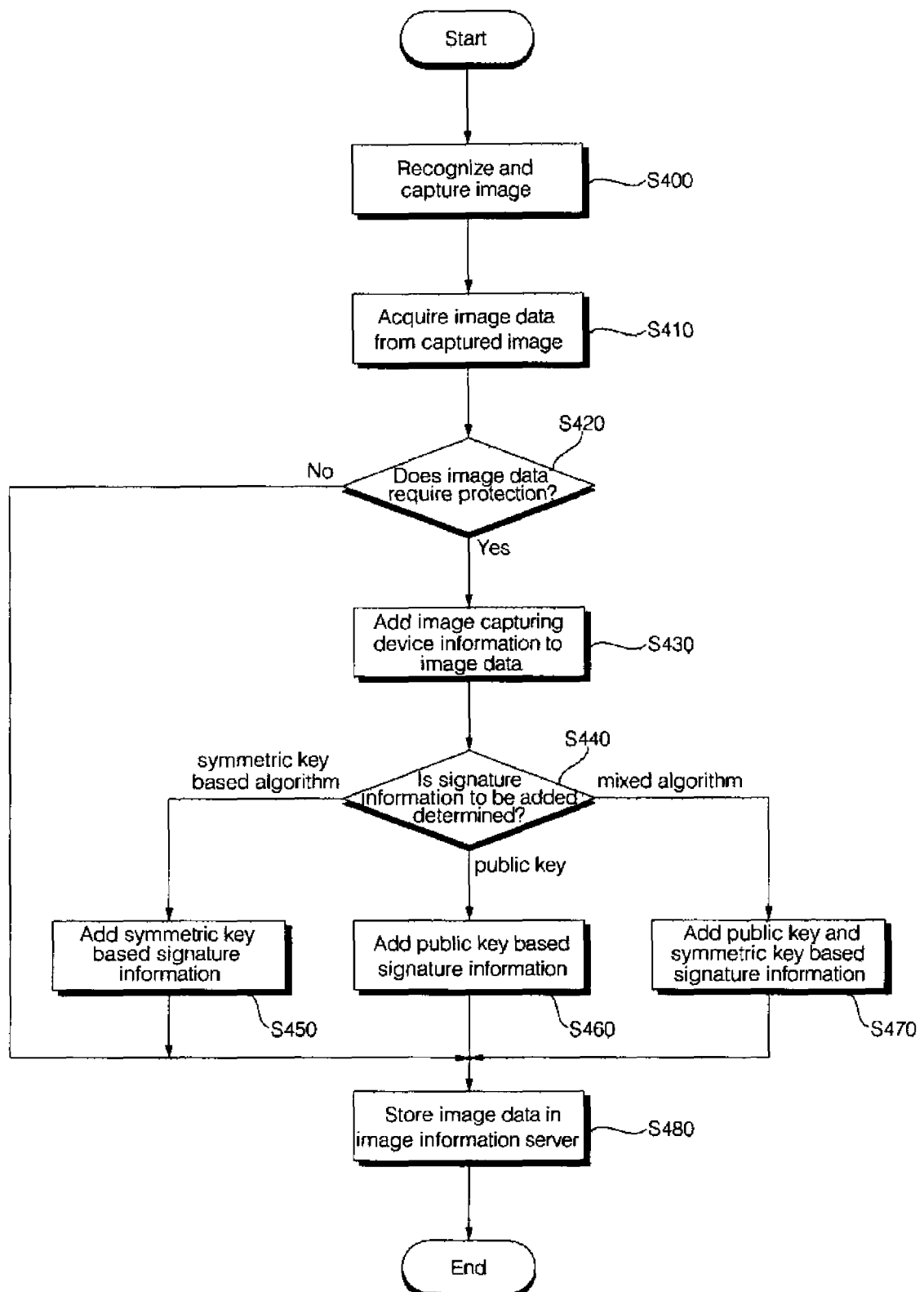
[Fig. 2]



[Fig. 3]



[Fig. 4]



A. CLASSIFICATION OF SUBJECT MATTER***H04N 5/265(2006.01)i***

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8, H04N 7/167, H04L 9/00, G06K 9/00

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

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

WPI, e-Korean Intellectual Property Office Patent Search System.

KEYWORDS : image, capture, signature, public, symmetric, and key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006/0047966 A1 (Canon Kabushiki Kaisha (JP)), Mar.02,2006 Abstract The paragraphs [0067]~[0082] in the detailed description Fig.5 ~ fig.7 Claim 1	1-22
Y	US 2003/0123699 A1 (Canon Kabushiki Kaisha, (JP)), Jul.03,2003 Abstract The paragraphs [0068]~[0095] in the detailed description Fig.6 ~ fig.8 Claims 1, 6, and 7	1-22
A	KR 10-2007-0026930 A (BSTECH CO., LTD.(KR)), Mar.09,2007 Abstract The paragraphs related to the fig.4~fig.5 in the detailed description Fig.4~fig.5 Claim 1	1-22



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

26 DECEMBER 2008 (26.12.2008)

Date of mailing of the international search report

26 DECEMBER 2008 (26.12.2008)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-
gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

PARK, Sung Ho

Telephone No. 82-42-481-5743



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2008/005399

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006/0047966 A1	Mar .02 .2006	None	
US 2003-0123699 A1	03.07.2003	CN 1430411 A	16.07.2003
		EP 1326424 A2	09.07.2003
		EP 1326424 A3	08.09.2004
		EP 1326424 A2	09.07.2003
		JP 2003-198540 A	11.07.2003
		KR 10-2003-0057480	04.07.2003
KR 10-2007-0026930 A	Mar .09 .2007	None	