(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 March 2007 (29.03.2007)

PCT

(10) International Publication Number
WO 2007/035062 A1

(51) International Patent Classification:
G06F 11/00 (2006.01)

(21) International Application Number:
PCT/KR2006/003781

(22) International Filing Date:
22 September 2006 (22.09.2006)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2005-0088361
22 September 2005 (22.09.2005) KR
10-2006-0091932
21 September 2006 (21.09.2006) KR

(71) Applicant *(for all designated States except US)*: **KT CORPORATION** [KR/KR]; 206, Jungja-dong, Bundang-gu, Seongnam-city, Kyeonggi-do 463-711 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KIM, Jong-Heum** [KR/KR]; 17, Umyeon-dong, Seocho-gu, Seoul 137-140 (KR). **KIM, Jong-An** [KR/KR]; 17, Umyeon-dong, Seocho-gu, Seoul 137-140 (KR). **HAN, Pyong-Hee** [KR/KR]; 17, Umyeon-dong, Seocho-gu, Seoul 137-140 (KR).

(74) Agent: **SHINSUNG PATENT FIRM**; 2-3F, Line Bldg., 823-30, Yeoksam-dong, Kangnam-ku, Seoul 135-080 (KR).

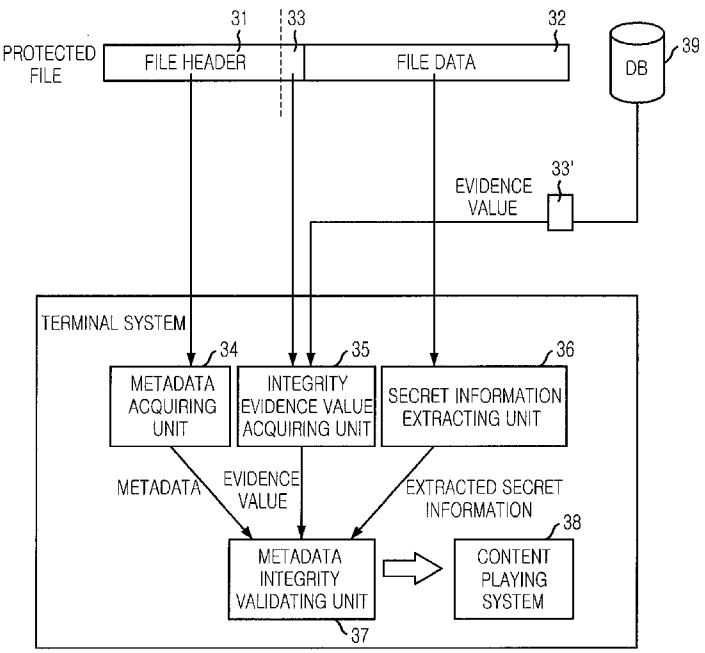
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, 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, 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, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, 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*

[Continued on next page]

(54) **Title:** METHOD FOR GENERATING STANDARD FILE BASED ON STEGANOGRAPHY TECHNOLOGY, AND APPARATUS AND METHOD FOR VALIDATING INTEGRITY OF METADATA IN THE STANDARD FILE



(57) **Abstract:** An apparatus for validating integrity of metadata in a standard file includes: a metadata acquiring unit for acquiring metadata from a protected file; an integrity evidence value acquiring unit for acquiring an integrity evidence value from a file or a database; a secret information extracting unit for extracting secret information of a file data; and a metadata integrity validating unit for checking if the metadata is correct by using the acquired metadata, the acquired integrity evidence value, and the extracted secret information.

WO 2007/035062 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD FOR GENERATING STANDARD FILE BASED ON STEGANOGRAPHY TECHNOLOGY, AND APPARATUS AND METHOD FOR VALIDATING INTEGRITY OF METADATA IN THE STANDARD FILE

Description

Technical Field

The present invention relates to a method for generating a standard file based on a steganography technology, an apparatus and method for validating integrity of metadata in the standard file, and a computer-readable recording medium storing a program for realizing the methods. More specifically, integrity evidence value of metadata is inserted into a file according to various standard file formats, and integrity, authentication, and non-repudiation for the inserted metadata are provided.

Background Art

International/domestic standard groups select parts considered as being necessary for industry activation in the respective fields, and a standard committee consisting of expert groups progresses the standardization. The standardized contents are made in a standard document and are officially published. Therefore, anyone who understands the standard can obtain the file information based on the standard document.

The standardization can attribute to the industry activation by supporting the interface between systems, but it is vulnerable to security attacks. As information technology (IT) industries are advanced, data are increasing and more complicated. For this reason, convenient search and storage are increasingly demanded. Thus, standardization and database of metadata draw

attraction. A system requiring a security manages the metadata using a separate security management system.

The metadata is a descriptor for describing data, or information for managing data. The metadata includes various types of data according to usage of data. The metadata may be systemically managed using database or may be inserted into a file header. Consequently, a service is made by combining metadata of the file and metadata of the database. The metadata stored in the database can be protected by a service provider, while the metadata contained in the file can be easily forged or falsified by anyone who understands its file structure. Therefore, the permanent relationship between file data and its metadata cannot be ensured, and thus it is necessary to protect important metadata inserted into the file. To solve these problems, a steganography technology has been developed which hides metadata inside the file data. According to the steganography technology, however, an amount of data that can be hidden is limited and it takes much time to extract it. Therefore, the steganography technology has difficulty in practical applications.

To overcome the difficulty, there is a demand for a method for ensuring integrity of metadata inserted into an opened standard file format using a steganography scheme and an encryption scheme.

Disclosure

Technical Problem

It is, therefore, an object of the present invention to provide an apparatus and method for validating integrity of metadata in a standard file using a steganography technology, and a computer-readable recording medium storing a program for realizing the

methods. Specifically, the integrity of the metadata inserted into a protected file, the authentication and non-repudiation of a protection subject, and the access control are provided. Thus, the permanent relationship of the metadata inside/outside the file and the service coherence can be obtained and various terminal-based business models can be implemented.

It is another object of the present invention to provide a method for generating a standard file and a computer-readable recording medium storing a program for realizing the method. Secret information is inserted into an original file or calculated from file data or contents according to a predetermined formula, and the integrity evidence value of the metadata is generated to thereby create the protected file.

Technical Solution

In accordance with one aspect of the present invention, there is provided an apparatus for validating integrity of metadata in a standard file, including: a metadata acquiring unit for acquiring metadata from a protected file; an integrity evidence value acquiring unit for acquiring an integrity evidence value from a file or a database; a secret information extracting unit for extracting secret information of a file data; and a metadata integrity validating unit for checking if the metadata is correct by using the acquired metadata, the acquired integrity evidence value, and the extracted secret information.

In accordance with another aspect of the present invention, there is provided a method for validating integrity of metadata in a standard file, including the steps of: a) acquiring metadata from a protected file when generation and consumption of the protected file are

requested, acquiring an integrity evidence value from a file or a database, and extracting secret information of a file data; and b) checking if the metadata is correct by using the acquired metadata, the acquired integrity evidence value, and the extracted secret information.

The method may further include the step of inserting secret information into an original file or calculating secret information from the file data or contents according to a predetermined formula, and generating the integrity evidence value of the metadata, thereby generating the protected file.

In accordance with a further aspect of the present invention, there is provided a method for generating a standard file, including the steps of: a) inserting a previously assigned inherent secret information into file data or contents, or calculating secret information from the file data or contents according to a predetermined formula; and b) inserting the metadata into a file header or optional field; and c) calculating the integrity evidence value of the metadata based on the metadata and the inherent code value or secret information, and inserting the calculated integrity evidence value into the file or separately managing the calculated integrity evidence value in a database of a server.

In accordance with a further aspect of the present invention, there is provided a computer-readable recording medium storing a program for realizing a method for validating integrity of metadata in a standard file, the method including the steps of: a) acquiring metadata from a protected file when generation and consumption of the protected file are requested, acquiring an integrity evidence value from a file or a database, and extracting secret information of a file data; and b) checking if the metadata is correct by using the acquired metadata, the acquired integrity evidence value, and the extracted

secret information.

The computer-readable recording medium may further include the step of inserting secret information into an original file or calculating secret information from the file data or contents according to a predetermined formula, and generating the integrity evidence value of the metadata, thereby generating the protected file.

In accordance with a further aspect of the present invention, there is provided a computer-readable recording medium storing a program for realizing a method for generating a standard file, the method including the steps of: a) inserting a previously assigned inherent secret information into a file data or contents, or calculating secret information from the file data or contents according to a predetermined formula; and b) inserting the metadata into a file header or optional field; and c) calculating the integrity evidence value of the metadata based on the metadata and the inherent code value or secret information, and inserting the calculated integrity evidence value into the file or separately managing the calculated integrity evidence value in a database of a server.

Advantageous Effects

In accordance with the present invention, the integrity of metadata inserted into an opened file format, authentication and non-repudiation of a subject, and access control can be provided, thereby obtaining the reliability of the metadata inserted into a file. The permanent relationship of the metadata existing inside/outside the file can be obtained and the service coherence can be maintained, thereby obtaining high service security.

Because the reliability of the metadata in the

opened file format can be obtained, the vulnerability in the standard such as DRM file format having the important service metadata can be overcome.

Moreover, because the metadata is reliable, a server initiative service using the metadata stored in a database of a server and a terminal initiative service model using metadata of a file can be provided. Therefore, various transaction models between terminals can be surely supported.

Description of Drawings

The above and other objects and features of the present invention will become apparent from the following description of the preferred embodiments given in conjunction with the accompanying drawings, in which:

Fig. 1 illustrates a process of generating a standard file (a protected file) by inserting secret information into an original file or calculating secret information from file data (contents) according to a predetermined formula;

Fig. 2 illustrates a standard file (a protected file) having an integrity evidence value inserted into an original file in accordance with an embodiment of the present invention; and

Fig. 3 illustrates an apparatus for validating integrity of metadata in a standard file in accordance with an embodiment of the present invention.

Best Mode for the Invention

Other objects and aspects of the invention will become apparent from the following description of the embodiments with reference to the accompanying drawings, which is set forth hereinafter.

Fig. 1 illustrates a process of generating a standard file (a protected file) by inserting secret information into an original file or calculating secret information from file data (contents) according to a predetermined formula, and Fig. 2 illustrates a standard file (a protected file) having an integrity evidence value inserted into an original file in accordance with an embodiment of the present invention.

A file generated based on a standard file format can be arbitrarily analyzed by anyone understanding its standard. Thus, data can be read and a desired data can be inserted. This means not only the enhanced compatibility but also the security vulnerability.

To solve the security vulnerability, a steganography technology such as watermarking or fingerprinting is developed. According to this technology, secret codes are inserted into file contents so that their relationship can be kept on. In recent years, technologies robust to various attacks have been developed.

The steganography technology uses the feature of contents. For example, frequency components of image or audio are analyzed and secret information is inserted. Therefore, if encrypted contents lose features, secret information cannot be inserted into the encrypted contents by using the steganography technology. In this case, another steganography technology is applied which calculates secret information from encrypted file data or contents according to a predetermined formula.

If the secret information of the file data is exposed to malicious users, the present invention becomes useless. Thus, the secret information to be hidden or the secret information calculated from the file data must be well managed so that they cannot be exposed to malicious persons. Algorithm and mechanism for generating a

protected file or extracting secret information from the protected file and their related source codes must be well managed so that they cannot be exposed to general persons.

The predetermined formula may be the selection of a specific area of a file data defined by the program or the combination of several areas and may be the result value obtained by performing a cryptographic hash or polynomial operation on the selected area.

In the case of the encrypted file, audio or video features of the original contents are all lost by the encryption. Therefore, the watermarking or fingerprinting cannot be applied to the encrypted contents. In order to generate an integrity evidence value for the encrypted contents, the formula defined in the encrypted file data is applied. The formula includes the calculation of secret information using file data transform, e.g., hash, polynomial operation, substitution, and permutation.

The present invention is directed to ensure integrity, access control, authentication and non-repudiation with respect to metadata inserted into a file header or an optional field by using steganography technology, digital signature, or keyed hash message authentication code (HMAC) value.

A security system inserts inherent code or secret information using the steganography technology, or calculates secret information from file data or contents according to the predetermined formula. Desired metadata is inserted into the file header or optional field. The digital signature value or HMAC value is calculated using the metadata or inherent code value and is inserted into the optional field of the file or managed as separate information.

The code or secret information is extracted using

the steganography technology, and the digital signature is verified or HMAC value is calculated using the code and the inserted metadata. In this way, the metadata inserted into the file can be easily verified.

The present invention provides a technology for integrity, access control, authentication and non-repudiation with respect to the file contents and their metadata and can be used when high security of the file contents is required.

One example of a DRM system for digital image is forgery/falsification prevention and authentication of passport photography.

When a digital passport issue system is implemented using the method of the present invention, an applicant inputs his/her identity information in an application and attaches a passport photograph. At this point, integrity evidence value such as digital signature is included in the passport issue application in order to guarantee the identification of the identity information filled in the issue application and the attached passport photograph. If the secret information is not included in the passport photograph, malicious persons may use the passport photograph by stealth and make an improper use of the passport. However, when the secret information is inserted into the passport photograph or the calculated value is used as an input value for calculating the integrity evidence value by using the steganography technology of the present invention, the correct integrity evidence value cannot be generated because the malicious persons do not know the secret information. That is, the passport issue application and the passport photograph file, which are physically divided, can obtain a permanent relationship by the medium of integrity evidence value, just like one file that cannot be divided. The generated integrity evidence value is HMAC code value

or digital signature value having the secret information of the passport issue application and the passport photograph.

In this manner, the permanent relationship can be assigned to two physically divided files. Alternatively, the two files can be combined in one file or can be divided into more than three files. It should be noted that the number of the physical files is not significant in the present invention.

That is, the file and the file data or contents containing metadata may include two or more files. For example, several photographs may be attached to the application, or the photograph and moving pictures may be attached.

The case where the present invention is applied to the unencrypted contents, e.g., passport photograph, has been described. The case where the present invention is applied to encrypted contents will be described below.

When the passport photograph is encrypted, key management information such as content ID and access information (URL, port number, etc.) of a key management server, as well as the above-described passport issue application information, is also stored in order to decode the encrypted passport photograph. When the encrypted photograph is read, a user terminal program extracts the key management information from the file, transfers the extracted value to the server, and obtains a correct decryption key. If a malicious person alters a part of the key management information and requests a content decryption key to the server, system failure may occur due to a deny of service (DOS). In order to cope with the malicious attacks, the present invention assigns a permanent relationship to the encrypted passport file and the key management information and ensures the integrity. Therefore, when the information is

maliciously altered, a client program verifies it and disables the trial of the request to the server. Based on this principle, a redistribution business model can be provided more stably. In the retribution business model, the encrypted contents are distributed among users in a P2P form, and a content decryption key and license are received from a lawful user. Like the encrypted passport photograph, because the key management information for obtaining the decryption key of the contents is contained in the content file downloaded in a P2P form, the malicious users may alter the information. If the information is altered, the above-described problems are caused and the service reliability is badly affected.

In addition, the present invention can obtain the same effect with respect to audio/video/text contents and various file format contents, as well as the DRM system for the digital image. Consequently, the drawbacks of the standard DRM can be solved.

The present invention includes the process of generating the protected file as shown in Fig. 1 and the process of validating the integrity of metadata as shown in Fig. 3. In the process of Fig. 1, the secret information is inserted into the original file, or the secret information is calculated from the file data or contents, based on the predetermined formula. Then, the integrity value 33 of metadata is generated. In the process of Fig. 3, when the real terminal system uses the protected file, the integrity of metadata is validated.

In the process of generating the protected file or standard file, previously assigned inherent secret information is inserted into the file data or contents, or the secret information is calculated from the file data or contents, based on the predetermined formula. Then, the metadata is inserted into the file header or optional field, and the integrity evidence value of the

metadata, e.g., HMAC or digital signature value, is calculated based on the metadata and inherent code value or secret information. The calculated integrity evidence value is inserted into the optional field, or it is separately managed in the database of the server.

Through the above-described process, the protected file or standard file is generated and will be used in an apparatus for validating the integrity, which is shown in Fig. 3.

The standard file protected by inserting the code into the original file has a format of Fig. 2. The original file may be compressed using various kinds of multimedia compression technologies. The metadata or file header 21 of the protected file is identical to the original metadata. When the digital signature technology is used, the integrity evidence value 33 must contain the information related to the digital signature, distinguish name (DN). The integrity evidence value may be inserted into the file, as indicated by a reference numeral 23, or may be separately managed, as indicated by a reference numeral 24.

The steganography technology may be a complicated technology such as a watermarking scheme or fingerprinting scheme, or may be a simple technology such as the selection of a specific area of the file data defined by a program or a combination of several areas, or may be the result value obtained by performing a cryptographic hash or polynomial operation on the selected area.

Fig. 3 illustrates an apparatus for validating integrity of metadata in a standard file in accordance with an embodiment of the present invention. Specifically, Fig. 3 illustrates the process of playing the protected file in which the integrity evidence value 33 of the metadata is inserted in a terminal system.

Referring to Fig. 3, the apparatus or terminal system in accordance with the present invention includes a metadata acquiring unit 34, an integrity evidence value acquiring unit 35, a secret information extracting unit 36, and a metadata integrity validating unit 37. The metadata acquiring unit 34 acquires metadata 31 from the protected file in order to validate the integrity of metadata before the playing of the file or the operation of a content play system 38. The integrity evidence value acquiring value 35 acquires the integrity evidence value 33 from the file or the database 39 in order to validate the integrity of the metadata before the playing of the file. The secret information extracting unit 36 extracts the secret information of the file data in order to validate the integrity of the metadata before the playing of the file. The metadata integrity validating unit 37 checks if the metadata is correct by using the acquired metadata 31, the integrity evidence value 33, and the extracted secret information.

The file header 31 includes a variety of service information for services using the file, and management information such as service access URL, content ID, key management information, and content metadata. When the digital signature technology is used, the integrity evidence value 33 must include the information related to the digital signature, distinguish name (DN).

The file data 32 is the contents of the file containing the secret information that is inserted into audio/video/text information according to a predetermined algorithm.

The integrity evidence value 33 is HMAC or digital signature value obtained using the metadata and the secret information.

The database 39 represents a database server for separately managing the metadata integrity evidence value

33'. The database 39 must be always in the on-line state so that the terminal system can validate the integrity.

An operation of the apparatus for validating the integrity of the metadata in the standard file will be described below in detail.

In order for the terminal system to ensure the integrity of the metadata, the metadata 31 is inserted into the original file in a standard form. The secret information is inserted into the file data 32 or is calculated. The HMAC is generated using the inserted metadata and secret information. The HMAC is used as the evidence value. The evidence value may be inserted into the file and used in the verify operation, or may be stored in the database 39 and separately managed (33'). The evidence values 33 and 33' can also be obtained using the digital signature value. In this case, the signature message includes the metadata and the secret information. At this point, the distinguish name must be inserted into the metadata.

It is preferable to use a public key in order for higher security, depending on technical characteristics. The use of the HMAC can secure the integrity. However, if a malicious user extracts the secret information of other user and inserts the extracted secret information, the authentication and non-repudiation will be lost. On the contrary, the use of the digital signature can obtain the permanent relationship through the hidden code and can obtain the integrity, authentication, and non-repudiation through the digital signature. Thus, the above-described problem does not occur. Consequently, the digital signature scheme is more robust than the HMAC scheme. However, compared with the HMAC scheme, the digital signature scheme is difficult to implement and there are the items to be managed. Therefore, the HMAC scheme and the digital signature scheme must be

appropriately selected and applied, depending on the required security degree. The generated evidence value may be inserted into the file or may be transferred to the server and stored in the database 39.

In order to validate the integrity of the metadata 31, the terminal system acquires the evidence values 33 and 33', such as HMAC or digital signature value, from the file or the database 39. Then, the terminal system extracts the secret information according to the predetermined algorithm and checks if the evidence values are correct by comparing the HMAC value or verifying the digital signature value.

Using these characteristics, the terminal system performs the access control so that only the person who provides the correct evidence value, i.e., the packaging subject of the original file can modify the metadata of the completely packaged file. In some cases, the terminal system validates the integrity of the metadata in order to consume the protected file, reads other information from the server by using the verified metadata information, and performs other operation. Thus, much time is taken in the terminal system. Therefore, in order to appropriately adjust the tradeoff between the necessary time and the security degree, an appropriate steganography technology is selected and designed depending on file formats, e.g., image, audio/video, text, etc.

The methods in accordance with the embodiments of the present invention can be realized as programs and stored in a computer-readable recording medium that can execute the programs. Examples of the computer-readable recording medium include CD-ROM, RAM, ROM, floppy disks, hard disks, magneto-optical disks and the like.

The present application contains subject matter related to Korean patent application No. 2005-0088361,

and No. 2006-0091932 filed in the Korean Intellectual Property Office on September 22, 2005, and on September 21, 2006, the entire contents of which is incorporated herein by reference.

While the present invention has been described with respect to certain preferred embodiments, it will be apparent to those skilled in the art that various changes and modifications may be made without departing from the scope of the invention as defined in the following claims.

What is claimed is:

1. An apparatus for validating integrity of metadata in a standard file, comprising:

a metadata acquiring unit for acquiring metadata from a protected file;

an integrity evidence value acquiring unit for acquiring an integrity evidence value from a file or a database;

a secret information extracting unit for extracting secret information of a file data; and

a metadata integrity validating unit for checking if the metadata is correct by using the acquired metadata, the acquired integrity evidence value, and the extracted secret information.

2. The apparatus as recited in claim 1, wherein the protected file is generated by inserting a previously assigned secret information into an original file or calculating secret information from a file data or contents according to a predetermined formula, and generating the integrity evidence value of the metadata.

3. The apparatus as recited in claim 2, wherein the predetermined formula is a selection of a specific area of a file data defined by a program or a combination of a plurality of areas, or a result value obtained by performing a secret information calculation through a transform of a file data using a cryptographic hash, polynomial operation, substitution, or permutation on the selected area.

4. The apparatus as recited in claim 3, wherein the integrity evidence value is calculated using a cryptographic scheme including a keyed hash message

authentication code (HMAC) and a digital signature obtained from metadata of a file header and secret information of the file data or contents, the integrity evidence value being added to an optional field of the file or managed as separate information in a database.

5. The apparatus as recited in claim 4, wherein HMAC is used to insert the previously assigned secret information into the original file or calculate secret information from the file data according to a predetermined formula and uses the secret information to generate the evidence value for the integrity of the metadata.

6. The apparatus as recited in claim 4, wherein the digital signature value is used to insert the previously assigned secret information into the original file or to calculate secret information from the file data or contents and uses the secret information to generate the evidence value for the integrity of the metadata, authentication of a subject generating the evidence value, non-repudiation, and data access control.

7. The apparatus as recited in claim 1, wherein the database is a database server for separately managing the metadata integrity evidence value, and maintains an on-line state in order for a terminal system to validate the integrity.

8. A method for validating integrity of metadata in a standard file, comprising the steps of:

a) acquiring metadata from a protected file when generation and consumption of the protected file are requested, acquiring an integrity evidence value from a file or a database, and extracting secret information of

a file data; and

b) checking if the metadata is correct by using the acquired metadata, the acquired integrity evidence value, and the extracted secret information.

9. The method as recited in claim 8, further comprising the step of inserting secret information into an original file or calculating secret information from the file data or contents according to a predetermined formula, and generating the integrity evidence value of the metadata, thereby generating the protected file.

10. The method as recited in claim 9, wherein the integrity evidence value is calculated using a cryptographic scheme including a keyed hash message authentication code (HMAC) and a digital signature obtained from metadata of a file header and secret information, the integrity evidence value being added to an optional field of the file or managed as separate information in a database.

11. The method as recited in claim 10, wherein the HMAC uses the secret information inserted by a steganography technology or calculated from the file data according to a predetermined formula to generate the integrity evidence value of the metadata.

12. The method as recited in claim 10, wherein the digital signature value enables the integrity of the metadata, authentication of a subject generating the evidence value, non-repudiation, and data access control.

13. A method for generating a standard file, comprising the steps of:

a) inserting a previously assigned inherent secret

information into file data or contents, or calculating secret information from the file data or contents according to a predetermined formula; and

b) inserting the metadata into a file header or optional field; and

c) calculating the integrity evidence value of the metadata based on the metadata and the inherent code value or secret information, and inserting the calculated integrity evidence value into the file or separately managing the calculated integrity evidence value in a database of a server.

14. The method as recited in claim 13, wherein the integrity evidence value is a keyed hash message authentication code (HMAC) obtained using the metadata of the file header and the secret information.

15. The method as recited in claim 13, wherein the integrity evidenced value is a digital signature value.

16. The method as recited in claim 15, wherein when a digital signature is used, a signature message includes the metadata and the secret information, a distinguish name being inserted in the metadata together with metadata of an original file.

17. A computer-readable recording medium storing a program for realizing a method for validating integrity of metadata in a standard file, the method comprising the steps of:

a) acquiring metadata from a protected file when generation and consumption of the protected file are requested, acquiring an integrity evidence value from a file or a database, and extracting secret information of a file data; and

b) checking if the metadata is correct by using the acquired metadata, the acquired integrity evidence value, and the extracted secret information.

18. The computer-readable recording medium as recited in claim 17, wherein the method further comprises the step of inserting secret information into an original file or calculating secret information from the file data or contents according to a predetermined formula, and generating the integrity evidence value of the metadata, thereby generating the protected file.

19. A computer-readable recording medium storing a program for realizing a method for generating a standard file, the method comprising the steps of:

a) inserting a previously assigned inherent secret information into a file data or contents, or calculating secret information from the file data or contents according to a predetermined formula; and

b) inserting the metadata into a file header or optional field; and

c) calculating the integrity evidence value of the metadata based on the metadata and the inherent code value or secret information, and inserting the calculated integrity evidence value into the file or separately managing the calculated integrity evidence value in a database of a server.

FIG. 1

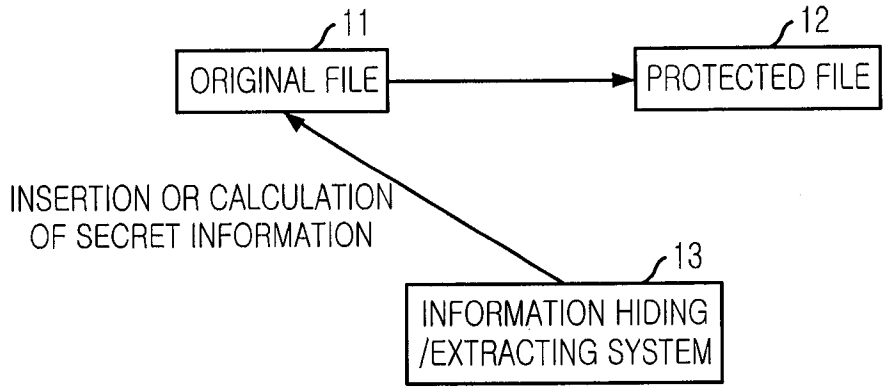

11
ORIGINAL FILE
12
PROTECTED FILE
INSERTION OR CALCULATION
OF SECRET INFORMATION
13
INFORMATION HIDING
/EXTRACTING SYSTEM

FIG. 2

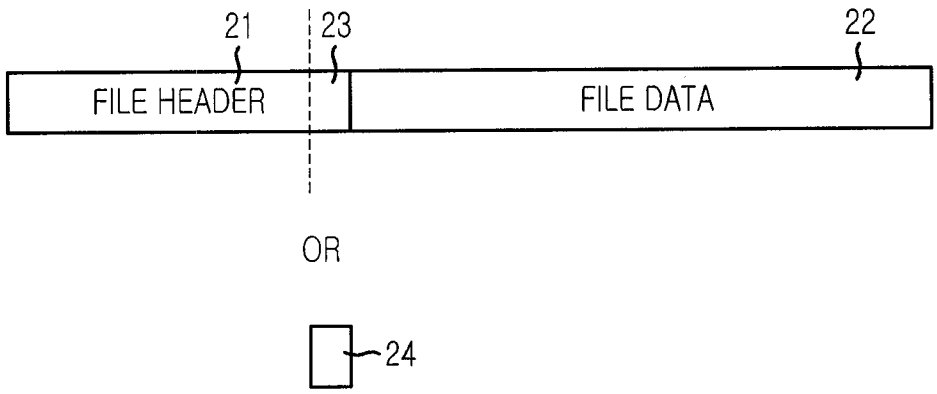
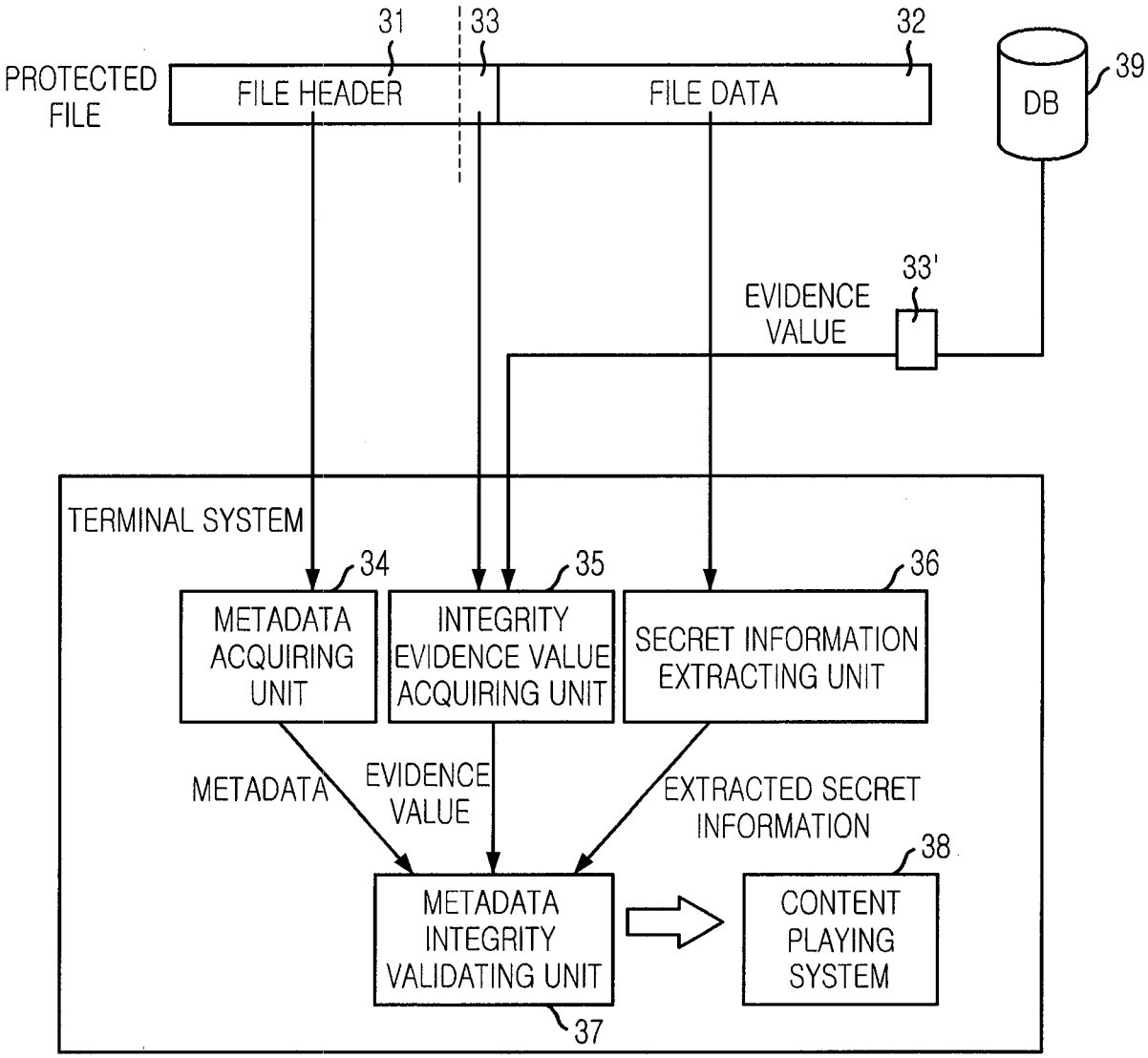

21
23
22
FILE HEADER
FILE DATA
OR
24

FIG. 3


PROTECTED FILE
31
33
32
FILE HEADER
FILE DATA
DB
39
33'
EVIDENCE VALUE
TERMINAL SYSTEM
34
35
36
METADATA ACQUIRING UNIT
INTEGRITY EVIDENCE VALUE ACQUIRING UNIT
SECRET INFORMATION EXTRACTING UNIT
METADATA
EVIDENCE VALUE
EXTRACTED SECRET INFORMATION
38
METADATA INTEGRITY VALIDATING UNIT
CONTENT PLAYING SYSTEM
37

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2006/003781

A. CLASSIFICATION OF SUBJECT MATTER

G06F 11/00(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 : G06F

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

KR, JP IPC as above

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

eKIPASS (KIPO internal) "metadata", "integrity", "secret", "hash"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US2002/0002468 A1 (International Business Machines Corp.) 03 Jan. 2002 See the abstract; claims1-16 ; figures 1d, 5	1-19
A	US2003/0046238 A1 (Sony Corp.) 06 Mar. 2003 See the abstract; figure4	1-19
A	US6389403 B1 (International Business Machines Corp.) 14 May. 2002 See the abstract; figure1A-1D	1-19
A	KR10-2004-0034165 (Electronics and Telecommunications Research Institute) 28 Apr. 2004 See the abstract; figure6	1-19

☐ 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	Date of mailing of the international search report
15 JANUARY 2007 (15.01.2007)	**15 JANUARY 2007 (15.01.2007)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

JEONG, Hae Kon

Telephone No. 82-42-481-5986

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR2006/003781

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US2002/0002468A1	03.01.2002	KR1020010050111A	15.06.2001
		AT340379E	15.10.2006
		DE60030814C0	02.11.2006
		EP01077398A1	21.02.2001
		IL137880A0	31.10.2001
		US2002107803A1	08.08.2002
		US20030105718A1	05.06.2003
		US6611812BB	26.08.2003
US2003/0046238A1	06.03.2003	CN1309487A	22.08.2001
		EP01130492A2	05.09.2001
		EP01130492A3	10.11.2004
		JP2001175606A2	29.06.2001
		KR2001082592A	30.08.2001
		TW559705B	01.11.2003
US6389403B1	14.05.2002	AU199954818A1	06.03.2000
		CA2338414AA	24.02.2000
		CA2467974AA	24.02.2000
		CA2467998AA	24.02.2000
		CN1163805C	25.08.2004
		CN1289100A	28.03.2001
		CN1320232A	31.10.2001
		EP01085443A2	21.03.2001
		EP01085443A3	05.01.2005
		IL140935A0	10.02.2002
		JP2001160003A2	12.06.2001
		KR2001050381A	15.06.2001
		TW222057B	11.10.2004
		TW454132B	11.09.2001
		W00008909A2	24.02.2000
KR1020040034165A	28.04.2004	NONE	