Description

METHOD AND PORTABLE STORAGE DEVICE FOR ALLOCATING SECURE AREA IN INSECURE AREA

Technical Field

[1] The present invention relates to a portable storage device, and more particularly, to a method for extending a secure area in a portable storage device and the portable storage device therefore.

Background Art

[2] A portable storage device is a removable device that stores and moves data of diverse digital devices such as mobile phones, computers, and digital cameras. The portable storage device includes a section for storing data and a section for performing operations and controls. A multimedia card (MMC) is a portable storage device that stores multimedia data to be used in diverse digital devices, exceeding the limits of conventional hard disks and compact discs. In addition, the MMC includes an operating section that is not present in conventional storage media, so that the MMC can perform control, encryption, and authentication in addition to storing data. As a result, the MMC is appropriate for storing a large amount of diverse multimedia data. Recently, a secure MMC for achieving security and protection of copyright in storage and transport of digital content has been developed by adding a security feature to the MMC, and therefore, protection of digital content has become possible. As the concept of digital rights management (DRM) on digital content is introduced, a security feature and an encryption feature for a rights object is needed and necessity of a portable storage device providing both of the security and encryption features arises. Hereinafter, digital devices such as digital cameras, mobile phones, computers, and digital camcorders are referred to as host devices.

[3] A portable storage device includes a secure area to protect stored data and prevent an unauthorized user or application from accessing or changing data. FIG. 1 illustrates the structure of a conventional portable storage device 10. The conventional portable storage device 10 includes a system area, 20, a secure area 30, and an insecure area 40. The system area 20 stores system information, version information, etc. The secure area 30 is formatted in a special file system and the insecure area 40 is formatted in a normal file system.

Disclosure of Invention

Technical Problem

[4] Conventionally, the size of a secure area is fixed and cannot be changed. As a result, when the amount of secure data to be stored in the secure area is large, all of the

secure data may not be stored in the secure area. To overcome the limit of the secure area having the fixed size, the size of the secure area has been changed through formatting. For this operation, a storage section of a portable storage device is divided into a secure area and an insecure area. The secure area is formatted in a special file system to provide a security feature and the insecure area is formatted in a normal file system such as File Allocation Table (FAT) 16 or a New Technology File System (NTFS). Reformatting is performed to change the size of the secure area.

[5] However, since formatting needs to be performed before the size of the secure area is changed, data needs to be backed up before the formatting and to be copied or moved to the portable storage device after the formatting.

Technical Solution

[6] Therefore, development of a method of extending a secure area without a data backup procedure and a portable storage device therefor is desired.

[7] The present invention provides a method and a portable storage device for easily extending a secure area in the portable storage device.

[8] The present invention also provides a method and portable storage device for allocating a secure area in an insecure area to protect data in the secure area without limit in the size of the secure area.

[9] According to an aspect of the present invention, there is provided a method of allocating a secure area in an insecure area of a portable storage device. The method includes allocating a secure area for storing data to be received within an insecure area; sending position information regarding the secure area allocated within the insecure area to a host device; receiving the position information and data to be stored in the secure area from a secure application of the host device; and encrypting and storing the data in the insecure area based on the position information.

[10] According to another aspect of the present invention, there is provided a method of allocating a secure area in an insecure area of a portable storage device, the method including receiving data to be stored in the secure area from a secure application of a host device, securing the secure area for storing the data within the insecure area and encrypting and storing the data in the secure area, and sending a result of storing the data to the host.

[11] According to still another aspect of the present invention, there is provided a portable storage device for allocating a secure area in an insecure area, the portable storage device including a storage section comprising an insecure area and a secure area, a transmitter sending position information regarding the secure area of the storage section to a host device, a receiver receiving the position information and data to be stored in the secure area from the host device, and a secure application encrypting and storing the data in the storage section based on the position information.

Description of Drawings

[12] The above and other aspects of the present invention will become more apparent by describing in detail exemplary embodiments thereof with reference to the attached drawings in which:

[13] FIG. 1 illustrates the structure of a conventional portable storage device;

[14] FIG. 2 illustrates the structure of a portable storage device having an insecure area including a secure area, according to an exemplary embodiment of the present invention;

[15] FIG. 3 illustrates a procedure of storing data in a secure area of a portable storage, according to an exemplary embodiment of the present invention;

[16] FIG. 4 illustrates the structure of a mapping table existing in a portable storage device, according to an exemplary embodiment of the present invention;

[17] FIG. 5 illustrates a procedure of blocking an unauthorized access to the secure area, according to an exemplary embodiment of the present invention;

[18] FIG. 6 is a functional block diagram of a portable storage device, according to an exemplary embodiment of the present invention;

[19] FIG. 7 is a flowchart of a method of storing and accessing data in a portable storage device, according to an exemplary embodiment of the present invention; and

[20] FIG. 8 is a flowchart of a method of storing and accessing data in a portable storage device, according to another exemplary embodiment of the present invention.

Mode for Invention

[21] Advantages and features of the present invention and methods of accomplishing the same may be understood more readily by reference to the following detailed description of exemplary embodiments and the accompanying drawings. The present invention may, however, be embodied in many different forms and should not be construed as being limited to the exemplary embodiments set forth herein. Rather, these exemplary embodiments are provided so that this disclosure will be thorough and complete and will fully convey the concept of the invention to those skilled in the art, and the present invention will only be defined by the appended claims. Like reference numerals refer to like elements throughout the specification.

[22] A method of allocating a secure area in an insecure area of a portable storage device and a portable storage device providing the method according the present invention will be described hereinafter with reference to flowchart illustrations of methods according to exemplary embodiments of the invention. It will be understood that each block of the flowchart illustrations, and combinations of blocks in the flowchart illustrations, can be implemented by computer program instructions. These computer program instructions can be provided to a processor of a general purpose

computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which are executed via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions specified in the flowchart block or blocks.

[23] These computer program instructions may also be stored in a computer usable or computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer usable or computer-readable memory produce an article of manufacture including instruction means that implement the function specified in the flowchart block or blocks.

[24] The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implemented process such that the instructions that are executed on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block or blocks.

[25] And each block of the flowchart illustrations may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that in some alternative implementations, the functions noted in the blocks may occur out of the order. For example, two blocks shown in succession may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved.

[26] FIG. 2 illustrates the structure of a portable storage device 100 having an insecure area 400 including a secure area, according to an exemplary embodiment of the present invention. The portable storage device 100 is connected to a host device 900. The host device 900 may be a notebook computer, a mobile phone, a personal digital assistant (PDA), or an MP3 player and communicates with the portable storage device 100 through a secure application 950. The portable storage device 100 includes a secure application 500, a system area 200, a read-only secure area 300, and an insecure area 400. The system area 200 stores information on a system. The read-only secure area 300 can by accessed by only an application that has been authenticated by the portable storage device 100. Data related with security is usually stored in the read-only secure area 300 when the portable storage device 100 is manufactured or before it is on the market. The data cannot be changed or removed.

[27] Data can be freely stored in and read from the insecure area 400. The insecure area 400 includes a plurality of readable/writable secure areas 311, 312, and 313. Accordingly, a secure area can be created in the insecure area 400 and data can be stored

in the secure area, through the secure application 500. The data stored in the secure area in the insecure area 400 can be read through the secure application 500.

[28] Operations performed to store security data in and read security data from the insecure area 400 according to an exemplary embodiment of the present invention will be described with reference to FIG. 2. In operation S11, the host device 900 secures space in the insecure area 400 of the portable storage device 100 through the secure application 950 according to the mechanism of a file system of the insecure area 400. This operation is the same as an operation of storing data in a File Allocation Table (FAT) 16/32. The secured space becomes a readable/writable secure area. In operation S12, the secure application 950 receives an address value of the secured space.

[29] In operation S13, the secure application 950 of the host device 900 sends the address value and data to be stored in a secure area to the secure application 500 of the portable storage device 100. The secure application 500 of the portable storage device 100 may include a table for mapping the address value of the secure area existing in the insecure area 400 to a relative address value that the secure application 500 can recognize. In operation S14, the secure application 500 stores the received data to a corresponding address. The data is protected through a protection technique such as encryption before being stored.

[30] The data stored in the secure area secured in the insecure area 400 through operations S11 through S14 can be read, removed, or updated through the secure application 500.

[31] The secure application 950 of the host device 900 sends a command to read, update, or remove data stored in the readable/writable secure area 312 together with an identification of the data. When the secure application 950 of the host device 900 is normally authenticated, the secure application 500 of the portable storage device 100 accesses the readable/writable secure area 312 having the identification and reads, updates, or removes the data in the readable/writable secure area 312. Since the stored data has been encrypted, decryption is performed when the data is read and then the read data is sent to the host device 900.

[32] Operations performed to store security data in the insecure area 400 according to another exemplary embodiment of the present invention will be described with reference to FIG. 3. Operations of creating the secure area in the insecure area 400 are the same as those illustrated in FIG. 2. Unlike the operations illustrated in FIG. 2, the host device 900 sends data to be stored and information indicating that the data will be stored in a secure area to the portable storage device 100 in operation S21. The portable storage device 100 searches the insecure area 400 for space, e.g., the readable/writable secure area 312, in which the data can be stored and stores the received data in operation S22. The data is encrypted before being stored in the secure area. The

portable storage device 100 informs the host device 900 that the data has been stored in the secure area in operation S23.

[33] The data stored in the secure area created in the insecure area 400 through operations S21 through S23 can be read, removed, or updated through the secure application 500, as described above.

[34] For the security of transmitted and received commands and data when the data is input into or output from a secure area created in the insecure area 400 as described with reference to FIGS. 2 and 3, the data and the commands may be encrypted using an encryption method or key agreed between the secure application 950 of the host device 900 and the secure application 500 of the portable storage device 100.

[35] FIG. 4 illustrates the structure of a mapping table 510 existing in a portable storage device, according to an exemplary embodiment of the present invention. The mapping table 510 includes data identifier, a hash value of file position, and file position. The data identifier is needed by a host device accessing data stored in a secure area. When a particular application of the host device sends a data identifier, a secure application verifies whether the particular application has been authenticated. After the authentication of the particular application, a position where data indicated by the data identifier is stored is extracted from a file position item and the data stored in the secure area within an insecure area can be accessed based on the extracted position information. Since the data has been encrypted when stored in the secure area, decryption is needed to access the data and send it to the host device. External access to information on the file position is prohibited and the data is encrypted when stored in the secure area, so that the data in the secure area can be protected from external, unauthorized access.

[36] A hash value is sent in the same manner as the file identification. The hash value hinders the host device from recognizing a physical position where the data is stored, thereby preventing the direct access of the host device. In FIG. 2, position information sent to the secure application 950 of the host device 900 may be a hash value. In this case, the secure application 950 of the host device 900 sends a hash value and data to be stored to the portable storage device 100. Then, the secure application 500 of the portable storage device 100 can obtain position information corresponding to the hash value from the mapping table 510.

[37] FIG. 5 illustrates a procedure of blocking an unauthorized access to the secure area, according to an exemplary embodiment of the present invention. An insecure application 990 may access data in the secure area 311, 312, or 313 without authentication. The insecure application 990 may access the secure area 311, 312, or 313 within the insecure area 400 randomly or by extracting position information. However, even if the insecure application 990 tries to access data in the readable/writable secure

area 311 using the position information, since the data stored in the readable/writable secure area 311 has been encrypted, the insecure application 990 cannot read the data. As a result, the insecure application 990 cannot access the data stored in the readable/ writable secure area 311 within the insecure area 400.

[38] Unlikely, when the insecure application 990 tries to access data in the insecure area 400 using a data identifier stored in a secure area or a data identifier that the secure application 950 has received through the secure application 500 of the portable storage device 100, the insecure application 990 cannot recognize the position of the data and thus cannot access the data. Recognizing a data position using a hash value or data identifier is possible through the secure application 500 of the portable storage device 100. However, the insecure application 990 cannot communicate with the secure application 500 of the portable storage device 100, and therefore, it cannot access data in the readable/writable secure area 311, 312, or 313.

[39] FIG. 6 is a functional block diagram of a portable storage device, according to an exemplary embodiment of the present invention. The term 'module', as used herein, means, but is not limited to, a software or hardware component, such as a Field Programmable Gate Array (FPGA) or Application Specific Integrated Circuit (ASIC), which performs certain tasks. A module may advantageously be configured to reside on the addressable storage medium and configured to be executed on one or more processors. Thus, a module may include, by way of example, components, such as software components, object-oriented software components, class components and task components, processes, functions, attributes, procedures, subroutines, segments of program code, drivers, firmware, microcode, circuitry, data, databases, data structures, tables, arrays, and variables. The functionality provided for in the components and modules may be combined into fewer components and modules or further separated into additional components and modules. In addition, the components and modules may be implemented such that they are executed one or more CPUs in a communication system.

[40] The portable storage device 100 includes a receiver 141 and a transmitter 142 to receive and transmit data from and to the host device 900. A storage section 410 stores data in an insecure area and a secure area. As described above with reference to FIGS. 2 and 3, data to be stored in the secure area is encrypted. Since the storage section 410 stores both data for the insecure area and data for the secure area, data encrypted through the secure application 500 is stored in the secure area of the storage section 410. The secure application 500 stores data needed to be stored in the secure area in the storage section 410 and controls access to the data. The secure application 500 may keep security using the mapping table 510 illustrated in FIG. 4 and prohibit unauthorized access to the data by encrypting the data before storing it.

[41] The secure application 500 can perform authentication with the host device 900 and can perform operations related with the authentication using authentication, encryption and decryption features provided by an authentication section 160. The authentication section 160 provides features for encryption and decryption using a symmetric key algorithm or an asymmetric key algorithm and generates a session key. The features provided by the authentication section 160 perform a procedure of identifying and authenticating the host device 900 when the secure application 500 communicates with the host device 900 via a wired or wireless connection. In addition, the authentication section 160 provides authentication, encryption and decryption features to transport data between the secure application 950 of the host device 900 and the secure application 500 of the portable storage device 100 using a secure channel or mode.

[42] A secure area storage section 300 may be selectively provided. As described above with reference to FIGS. 2 and 3, when a secure area is positioned within an insecure area, read-only data may be separately stored in the secure area storage section 300. In addition, some readable/writable data may be stored in the secure area storage section 300. When no more space exists in the secure area storage section 300, space is secured in the insecure area of the storage section 410 and is used as a secure area. For example, the secure area storage section 300 may have a space of 50 Mbytes, the storage section 410 may have a space of 500 Mbytes, and the secure area storage section 300 may include both a read-only secure area and a readable/writable secure area. In this situation, when the secure area storage section 300 does not have empty space for storing data any more, a secure area may be secured in the storage section 410 and data may be stored therein.

[43] A ratio between an insecure area and a secure area and how the insecure area and the secure area will be provided may be different according to exemplary embodiments, and the present invention is not restricted to the exemplary embodiments described in this specification.

[44] FIG. 7 is a flowchart of a method of storing and accessing data in a portable storage device, according to an exemplary embodiment of the present invention. The flowchart shown in FIG. 7 implements the operations described with reference to FIG. 2. In operation S101, a command is received from a host device. If it is determined that the command is not for a secure area in operation S103, a request for an insecure area is processed in operation S105 and the method ends. If it is determined that the command requests to secure a space to store data in the secure area in operation S108, a secure application searches the insecure area for position information regarding the secure area to which relevant data having a certain size will be stored in operation S111. The position information is hashed or stored in a mapping table in operation

S112 in order to prevent an external, unauthorized user from directly accessing a corresponding position. The hashed position information or information for finding the position information in the mapping table is sent to the host device in operation S113.

[45] When the command does not include information about data size, it is determined whether the command requests to access data in operation S120. It is determined that the command does not request data access when the host device received the position information in operation S113 sends the position information together with data to be stored in the corresponding position. Accordingly, the data received from the host device is encrypted in operation S121. The encrypted data is stored in an area corresponding to the received position information in operation S122. An actual position of a secure area to which the data will be stored can be obtained from the received position information referring to a hash table or the mapping table.

[46] If it is determined that the command requests data access in operation S120, decryption needed to access data in a secure area will be performed. For the decryption, data is extracted from the secure area designated by position information in operation S125. Since the position information may have been changed using the hash table or the mapping table, an actual position of the secure area may be obtained using the hash table or the mapping table. The data extracted from the position is decrypted in operation S126. The command is executed on the data in operation S127.

[47] To store or access data in a secure area, an authentication procedure may be added. The authentication procedure can be performed through a secure application within the host device.

[48] FIG. 8 is a flowchart of a method of storing and accessing data in a portable storage device, according to another exemplary embodiment of the present invention. The flowchart illustrated in FIG. 8 implements the operations described with reference to FIG. 3. In operation S151, a command is received from a host device. If it is determined that the command is not for a secure area in operation S153, a request for an insecure area is processed in operation S155 and the method ends. If it is determined that the command requests to store data in the secure area in operation S158, a secure application secures a space as the secure area within the insecure area in operation S161. The data is encrypted and stored in the space secured as the secure area in operation S162. A result of storing the data is sent to the host device in operation S163. The storing result may include position information regarding the secure area to which the data has been stored. When the position information is sent, it may be changed using a hash function or a mapping table in order to prevent an unauthorized application from directly accessing a corresponding position.

[49] If it is determined that the command does not request to store data in operation S158, operations for accessing data will be performed. Data can be accessed using in-

formation regarding the data. When the information regarding the data includes position information, data in an area designated by the position information is extracted in operation S171. When the position information has been changed using the hash function or the mapping table, as described above, the secure area can be accessed using original position information. When the information regarding the data is not the position information but a data identifier, the position information can be identified using the mapping table 510 illustrated in FIG. 4. Data at a position corresponding to the position information is decrypted in operation S172. The command is executed on the decrypted data in operation S173.

[50] To store or access data in a secure area, an authentication procedure may be added. The authentication procedure can be performed through a secure application within the host device.

Industrial Applicability

[51] According to the present invention, a secure area can be easily extended in a portable storage device.

[52] In addition, data requiring security can be stored in an insecure area and the data stored in the insecure area can be protected from unauthorized access.

[53] It will be apparent to those skilled in the art that various modifications and changes may be made thereto without departing from the scope and spirit of the invention. Therefore, it should be understood that the above exemplary embodiments are not restrictive but illustrative in all aspects. The scope of the present invention is defined by the appended claims rather than the detailed description of the invention. All modifications and changes derived from the scope and spirit of the claims and equivalents thereof should be construed to be included in the scope of the present invention.

Claims

[1] A method of allocating a secure area in an insecure area of a storage device, the method comprising:
allocating a secure area for storing data to be received within an insecure area;
sending position information regarding the secure area allocated within the insecure area to a host device;
receiving the position information and data to be stored in the secure area from a secure application of the host device; and
encrypting and storing the data in the insecure area based on the position information.

[2] The method of claim 1, wherein the allocating of the secure area comprises:
receiving information regarding a size of the data from the host device; and
allocating the secure area having a sufficient size to store the data in the insecure area.

[3] The method of claim 1, further comprising changing the position information using a hash table or a mapping table.

[4] The method of claim 1, further comprising performing authentication with the secure application of the host device.

[5] The method of claim 1, further comprising:
receiving a request to access the data from the secure application of the host device;
extracting the data from the secure area within the insecure area and decrypting the data; and
sending the decrypted data to the host device.

[6] The method of claim 5, wherein the sending of the decrypted data comprises:
encrypting the decrypted data using a predetermined encryption method on which an agreement is made with the secure application of the host device; and
sending the encrypted data to the host device.

[7] A method of allocating a secure area in an insecure area of a storage device, the method comprising:
receiving data to be stored in the secure area from a secure application of a host device;
securing the secure area for storing the data within the insecure area and encrypting and storing the data in the secure area; and
sending a result of the storing the data to the host device.

[8] The method of claim 7, wherein the result of the storing the data comprises position information regarding the secure area storing the data within the

insecure area.

[9] The method of claim 8, further comprising changing the position information using a hash table or a mapping table.

[10] The method of claim 7, further comprising performing authentication with the secure application of the host device.

[11] The method of claim 7, further comprising:
receiving a request to access the data from the secure application of the host device;
extracting the data from the secure area within the insecure area and decrypting the data; and
sending the decrypted data to the host device.

[12] The method of claim 11, wherein the sending of the decrypted data comprises:
encrypting the decrypted data using a predetermined encryption method on which an agreement is made with the secure application of the host device; and
sending the encrypted data to the host device.

[13] A storage device for allocating a secure area in an insecure area, the storage device comprising:
a storage section comprising an insecure area and a secure area;
a transmitter which sends position information regarding the secure area of the storage section to a host device;
a receiver which receives the position information and data to be stored in the secure area from the host device; and
a secure application which encrypts and stores the data in the storage section based on the position information.

[14] The storage device of claim 13, wherein the secure application changes the position information using a hash table or a mapping table.

[15] The storage device of claim 13, wherein the secure application performs authentication with the host device.

[16] The storage device of claim 13, wherein the receiver receives a request to access the data from a secure application included in the host device, the secure application included in the storage device extracts the data from the secure area within the insecure area and decrypts the data, and the transmitter sends the decrypted data to the host device.

[17] The storage device of claim 16, wherein the secure application included in the storage device encrypts the decrypted data using a predetermined encryption method on which an agreement is made with the host device, and the transmitter sends the encrypted data to the host device.

[18] A storage device for allocating a secure area in an insecure area, the storage

device comprising:

a storage section comprising an insecure area and a secure area;

a receiver which receives data to be stored in the secure area of the storage section from a host device;

a secure application which secures a space for the secure area needed to store the data within the storage section, and encrypts and stores the data in the secure area; and

a transmitter which sends a result of the storing the data within the storage section to the host device.

[19] The storage device of claim 18, wherein the result of the storing the data comprises position information regarding the secure area storing the data within the insecure area.

[20] The storage device of claim 19, wherein the secure application changes the position information using a hash table or a mapping table.

[21] The storage device of claim 18, wherein the secure application performs authentication with the host device.

[22] The storage device of claim 18, wherein the receiver receives a request to access the data from the host device, the secure application extracts the data from the secure area within the insecure area and decrypts the data, and the transmitter sends the decrypted data to the host device.

[23] The storage device of claim 22, wherein the secure application encrypts the decrypted data using a predetermined encryption method on which an agreement is made with the host device.