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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2014 (23.01.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/012501 A1

(51) International Patent Classification:
G06F 21/00 (2013.01)

(21) International Application Number:
PCT/CN2013/079589

(22) International Filing Date:
18 July 2013 (18.07.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201210251187.3 19 July 2012 (19.07.2012) CN

(71) Applicant: **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN).

(72) Inventor: **LI, Danhua**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN).

(74) Agent: **BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.**; A-1-102, He Jing Yuan, Ji Men Li, Xueyuan Road, Haidian District, Beijing 100088 (CN).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, 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, KN, KP, KR, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: METHOD AND SYSTEM FOR RUNNING ENCRYPTED FILES

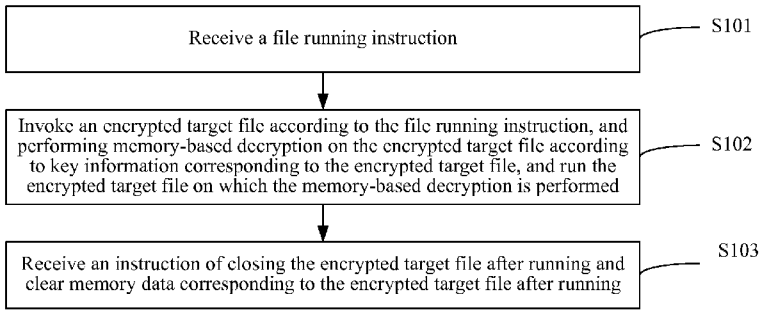


FIG. 1

(57) Abstract: A computer-implemented method for running an encrypted file and system are provided, where the method includes the following steps: receiving a file running instruction; invoking an encrypted target file according to the file running instruction, and performing memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file; and running the encrypted target file on which the memory-based decryption is performed.

WO 2014/012501 A1

METHOD AND SYSTEM FOR RUNNING ENCRYPTED FILES

RELATED APPLICATION

[0001] This application claims priority to Chinese Patent Application No. 201210251187.3, entitled "METHOD AND SYSTEM FOR RUNNING ENCRYPTED FILES," filed on July 19, 2012, which is incorporated by reference in its entirety.

TECHNICAL FIELD

[0002] The disclosed implementations relate generally to the field of computer security technologies, and in particular, to a file encryption and running method and a file encryption and running system.

BACKGROUND

[0003] With the increasing development and widespread application of computers, mobile phones, and other terminal electronic devices, security problems have caught increasing attention, and one kind of security is reflected in security protection on specific files (including software and so on). For the protection on the specific files, a manner currently adopted is described as follows: these files are encrypted through encryption/decryption software and so on; when a file needs to be run or is run, after a password of the encryption/decryption software is input correctly, a user finds a directory where an encrypted file is located; inputs a correct password of the file that needs to be run or is run; decrypts the file; and runs the file after the decryption is completed, or runs a file or software on which memory-based decryption is performed. Based on this manner, when a file on which memory-based decryption is performed needs to be run or is run, it is required to manually input a password of the file that needs to be run, and the file is run after password authentication is correct and the file is decrypted, which severely affects the efficiency of running of the encrypted file.

SUMMARY

[0004] For the problem existing in the prior art, the present invention is directed to provide a file encryption and running method and an encryption and running system, which can improve the efficiency when an encrypted file is run.

[0005] In order to achieve the objectives, the present invention adopts the following technical solutions:

[0006] A computer-implemented method for running an encrypted file is provided, which includes the following steps: receiving a file running instruction; invoking an encrypted target file according to the file running instruction, and performing memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file; and running the encrypted target file on which the memory-based decryption is performed.

[0007] A computer system for running an encrypted file is provided, which includes: a running instruction receiving unit, configured to receive a file running instruction; and a file running unit, configured to invoke an encrypted target file according to the file running instruction, perform memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed.

[0008] According to the solutions of the present invention, when it is required to run the encrypted target file, the key information corresponding to the encrypted target file is obtained, the memory-based decryption is performed on the encrypted target file in a memory by using the key information, and the encrypted target file is directly run after the memory-based decryption is completed. In this file running manner, the file can be opened and run without manually inputting a password of the encrypted target file and manually decrypting the file, thereby improving the efficiency of running the encrypted file. In another aspect, the encrypted target file is decrypted in the memory by using the key information, so that the decrypted file is stored in the memory without generating a permanent file, and therefore, it cannot be stolen by people, thereby improving the security of running the encrypted file.

BRIEF DESCRIPTION OF DRAWINGS

[0009] The aforementioned implementation of the invention as well as additional implementations will be more clearly understood as a result of the following detailed description of the various aspects of the invention when taken in conjunction with the drawings. Like reference numerals refer to corresponding parts throughout the several views of the drawings.

[0010] FIG. 1 is a schematic flowchart of Embodiment 1 of a file encryption and running method according to some embodiments of the present invention.

[0011] FIG. 2 is a schematic flowchart of Embodiment 2 of a file encryption and running method according to some embodiments of the present invention.

[0012] FIG. 3 is a schematic flowchart of Embodiment 3 of a file encryption and running method according to some embodiments of the present invention.

[0013] FIG. 4 is a schematic flowchart of Embodiment 4 of a file encryption and running method according to some embodiments of the present invention.

[0014] FIG. 5 is a block diagram of Embodiment 1 of a computer system according to some embodiments of the present invention.

[0015] FIG. 6 is a block diagram of Embodiment 2 of a computer system according to some embodiments of the present invention.

[0016] FIG. 7 is a block diagram Embodiment 3 of a computer system according to some embodiments of the present invention.

[0017] FIG. 8 is a block diagram Embodiment 4 of a computer system according to some embodiments of the present invention.

[0018] FIG. 9 is a block diagram illustrating a device in accordance with some embodiments of the present invention.

DETAILED DESCRIPTION

[0019] The following describes the solutions in the present invention in details in combination with exemplary embodiments. In the following illustration, embodiments of a file encryption and running method of the present invention are first illustrated, and then, embodiments of a file encryption and running system of the present invention are illustrated.

[0020] Embodiment 1

[0021] FIG. 1 shows a schematic flowchart of Embodiment 1 of a file encryption and running method according to some embodiments of the present invention. In this embodiment, a process of running an encrypted file is taken as an example for illustration.

[0022] As shown in FIG. 1, the file encryption and running method in Embodiment 1 includes the following steps:

[0023] Step S101: Receive a file running instruction.

[0024] Step S102: Invoke an encrypted target file according to the file running instruction, perform memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed.

[0025] According to the solution in this embodiment, when it is required to run the encrypted target file, the key information corresponding to the encrypted target file is obtained, the memory-based decryption is performed on the encrypted target file in a memory by using the key information, and the encrypted target file is directly run after the memory-based decryption is completed. In this file running manner, the file can be opened and run without manually inputting a password of the encrypted target file and manually decrypting the file, thereby improving the efficiency of running the encrypted file. In another aspect, the encrypted target file is decrypted in the memory by using the key information, so that the decrypted file is stored in the memory without generating a permanent file, and therefore, it cannot be stolen by people, thereby improving the security of running the encrypted file.

[0026] As shown in FIG. 1, in this embodiment, the following step is optionally further included:

[0027] Step S103: Receive an instruction of closing the encrypted target file after running and clear memory data corresponding to the encrypted target file after running.

[0028] Therefore, the encrypted target file that is run before does not leave relevant data information in the memory after the running encrypted target file is closed, so that information data relevant to the encrypted target file cannot be easily obtained by people, which further ensures the security of the encrypted target file.

[0029] In some embodiments, when the memory data is cleared, various manners are adopted according to different actual application requirements. In one implementation, after the instruction of closing the encrypted target file after running is received, a prompt about whether to clear the memory data is given, and a user selects whether to perform clearing. When it is determined that the clearing needs to be performed, the memory data is cleared based on a clearing instruction given by the user through selecting a corresponding option or button. In another implementation, a prompt is not given, and the memory data is directly and automatically cleared after the instruction of closing the encrypted target file after running is received, so as to enhance the security.

[0030] In addition, when the instruction of closing the encrypted target file after running is received, encryption is, optionally, further performed by directly invoking the key information corresponding to the encrypted target file, so that the encrypted target file after running does not need to be manually encrypted, thereby further improving the efficiency of running the encrypted file.

[0031] Embodiment 2

[0032] FIG. 2 shows a schematic flowchart of Embodiment 2 of a file encryption and running method according to some embodiments of the present invention. In this embodiment, the difference from the method in Embodiment 1 mainly lies in that the method in this embodiment is further described in combination with a file encryption process.

[0033] As shown in FIG. 2, the method in Embodiment 2 includes the following steps:

[0034] Step S201: Receive a file encryption instruction.

[0035] Step S202: Encrypt a file to be encrypted to obtain an encrypted target file, and generate key information corresponding to the encrypted target file.

[0036] Step S203: Store the key information and the corresponding encrypted target file.

[0037] Step S204: Receive a file running instruction.

[0038] Step S205: Invoke the encrypted target file according to the file running instruction, perform memory-based decryption on the encrypted target file according to the key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed.

[0039] According to the solution in this embodiment, when the file is encrypted, the key information corresponding to the encrypted target file is generated, and the key information and the encrypted target file are correspondingly stored, so that when it is required to run the encrypted target file, the corresponding key information thereof is directly obtained, and the encrypted target file is decrypted in a memory by using the key information. Therefore, the file can be opened and run without manually inputting a password of the encrypted target file and manually decrypting the file, thereby improving the efficiency of running the encrypted file. In another aspect, the encrypted target file is decrypted in the memory by using the key information, so that the decrypted file is stored in the memory without generating a permanent file, and therefore, it cannot be stolen by people, thereby further improving the security of running the encrypted file.

[0040] In some embodiments, when the key information and the encrypted target file are correspondingly stored, the key information and the encrypted target file are locally stored or stored in a remote server, or one of the key information and the encrypted target file is locally stored, and the other is stored in a remote server, and different settings are made according to different specific requirements. In another aspect, when the key information and the encrypted target file are locally stored or stored in the remote server, the key information and the encrypted target file are, optionally, combined into one file and stored, or the key information and the encrypted target file are stored as two separate files, so as to enhance the security, as long as a corresponding key relationship can be obtained based on the corresponding storage relationship to decrypt the encrypted target file, when the encrypted target file needs to be opened.

[0041] As shown in FIG. 2, in this embodiment, the following step is optionally further included:

[0042] Step S206: Receive an instruction of closing the encrypted target file after running and clear memory data corresponding to the encrypted target file after running.

[0043] Therefore, the encrypted target file that is run before does not leave relevant data information in the memory after the running encrypted target file is closed, so that information data relevant to the encrypted target file cannot be easily obtained by people, which further ensures the security of the encrypted target file.

[0044] In some embodiments, when the memory data is cleared, various manners are adopted according to different actual application requirements. In one implementation, after the instruction of closing the encrypted target file after running is received, a prompt about whether to clear the memory data is given, and a user selects whether to perform clearing. When it is determined that the clearing needs to be performed, the memory data is cleared based on a clearing instruction given by the user through selecting a corresponding option or button. In another implementation, prompt information is not given, and the memory data is directly and automatically cleared after the instruction of closing the encrypted target file after running is received, so as to enhance the security.

[0045] In addition, when the instruction of closing the encrypted target file after running is received, encryption is optionally further performed by directly invoking the key information corresponding to the encrypted target file, so that the encrypted target file after running does not need to be manually encrypted, thereby further improving the efficiency of running the encrypted file.

[0046] Embodiment 3

[0047] FIG. 3 shows a schematic flowchart of Embodiment 3 of a file encryption and running method according to some embodiments of the present invention. In this embodiment, the difference from Embodiment 1 mainly lies in that this embodiment is illustrated in combination with an identity authentication process.

[0048] As shown in FIG. 3, the file encryption and running method in Embodiment 3 includes the following steps:

[0049] Step S301: Receive an identity authentication instruction, and perform authentication on a user login identity.

[0050] Step S302: Obtain an encrypted target file list corresponding to the authenticated identity after the identity authentication succeeds.

[0051] Step S303: Receive a file running instruction through the encrypted target file list.

[0052] Step S304: Invoke an encrypted target file according to the file running instruction, perform memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed.

[0053] According to the solution in Embodiment 3, after the user identity authentication succeeds, a user that currently logs in or a user that needs to run an encrypted target file in the encrypted target file list is trusted, so that when it is required to run the encrypted target file, the corresponding key information thereof is directly obtained, and the encrypted target file is decrypted in a memory by using the key information. Therefore, the file can be opened and run without manually inputting a password of the encrypted target file and manually decrypting the file, thereby improving the efficiency of running the encrypted file. In another aspect, the encrypted target file is decrypted in the memory by using the key information, so that the decrypted file is stored in the memory without generating a permanent file, and therefore, it cannot be stolen by people, thereby improving the security of running the encrypted file.

[0054] In some embodiments, when the user identity is authenticated, various possible manners are adopted, for example, the identity authentication is performed according to information such as a numeric password, a facial image, fingerprint information, or audio data of a user, and a specific identity authentication manner is not elaborated herein.

[0055] As shown in FIG. 3, in this embodiment, the following step is optionally further included:

[0056] Step S305: Receive an instruction of closing the encrypted target file after running and clear memory data corresponding to the encrypted target file after running.

[0057] Therefore, the encrypted target file that is run before does not leave relevant data information in the memory after the running encrypted target file is closed, so that information data relevant to the encrypted target file cannot be easily obtained by people, which further ensures the security of the encrypted target file.

[0058] In some embodiments, when the memory data is cleared, various manners are adopted according to different actual application requirements. In one implementation, after the instruction of closing the encrypted target file after running is received, a prompt about whether to clear the memory data is given, and a user selects whether to perform clearing. When it is determined that the clearing needs to be performed, the memory data is cleared based on a clearing instruction given by the user through selecting a corresponding option or button. In another implementation, prompt information is not given, and the memory data is directly and automatically cleared after the instruction of closing the encrypted target file after running is received, so as to enhance the security.

[0059] In addition, when the instruction of closing the encrypted target file after running is received, encryption is optionally further performed by directly invoking the key information corresponding to the encrypted target file, so that the encrypted target file after running does not need to be manually encrypted, thereby further improving the efficiency of running the encrypted file.

[0060] Embodiment 4

[0061] FIG. 4 shows a schematic flowchart of Embodiment 4 of a file encryption and running method according to some embodiments of the present invention. In this embodiment, the difference from Embodiment 2 mainly lies in that this embodiment is illustrated in combination with an identity authentication process.

[0062] As shown in FIG. 4, the file encryption and running method in Embodiment 4 includes the following steps:

[0063] Step S401: Receive a file encryption instruction.

[0064] Step S402: Encrypt a file to be encrypted to obtain an encrypted target file, and generate key information corresponding to the encrypted target file.

[0065] Step S403: Store the key information and the corresponding encrypted target file.

[0066] Step S404: Receive an identity authentication instruction, and perform authentication on a user login identity.

[0067] Step S405: Obtain an encrypted target file list corresponding to the authenticated identity after the identity authentication succeeds.

[0068] Step S406: Receive a file running instruction through the encrypted target file list.

[0069] Step S407: Invoke the encrypted target file according to the file running instruction, perform memory-based decryption on the encrypted target file according to the key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed.

[0070] According to the solution in Embodiment 4, when the file is encrypted, the key information corresponding to the encrypted target file is generated, and the key information and the encrypted target file are correspondingly stored, so that when it is required to run the encrypted target file, the user identity is authenticated, and a user that currently logs in or a user that needs to run an encrypted target file in the encrypted target file list is trusted after the authentication succeeds. Therefore, when it is required to run the encrypted target file, the corresponding key information thereof is directly obtained, and the encrypted target file is decrypted in a memory by using the key information. Therefore, the file can be opened and run without manually inputting a password of the encrypted target file and manually decrypting the file, thereby improving the efficiency of running the encrypted file. In another aspect, the encrypted target file is decrypted in the memory by using the key information, so that the decrypted file is stored in the memory without generating a permanent file, and therefore, it cannot be stolen by people, thereby further improving the security of running the encrypted file.

[0071] In some embodiments, when the user identity is authenticated, various possible manners are adopted, for example, the identity authentication is performed according to

information such as a numeric password, a facial image, fingerprint information, or audio data of a user, and a specific identity authentication manner is not elaborated herein.

[0072] In this embodiment and the foregoing embodiments, when the user identity is authenticated, and the encrypted target file is decrypted in the memory, encryption/decryption software or a client that decrypts the encrypted target file may be adopted, and certainly, other possible manners may also be adopted, and a specific implementation manner is not elaborated herein.

[0073] As shown in FIG. 4, in this embodiment, the following step is optionally further included:

[0074] Step S408: Receive an instruction of closing the encrypted target file after running and clear memory data corresponding to the encrypted target file after running.

[0075] Therefore, the encrypted target file that is run before does not leave relevant data information in the memory after the running encrypted target file is closed, so that information data relevant to the encrypted target file cannot be easily obtained by people, which further ensures the security of the encrypted target file.

[0076] When the memory data is cleared, various manners are adopted according to different actual application requirements. In one implementation, after the instruction of closing the encrypted target file after running is received, a prompt about whether to clear the memory data is given, and a user selects whether to perform clearing. When it is determined that the clearing needs to be performed, the memory data is cleared based on a clearing instruction given by the user through selecting a corresponding option or button. In another implementation, prompt information is not given, and the memory data is directly and automatically cleared after the instruction of closing the encrypted target file after running is received, so as to enhance the security.

[0077] In addition, when the instruction of closing the encrypted target file after running is received, encryption is optionally further performed by directly invoking the key information corresponding to the encrypted target file, so that the encrypted target file after running does not need to be manually encrypted, thereby further improving the efficiency of running the encrypted file.

[0078] In addition, in the embodiment shown in FIG. 4, encryption on the file to be encrypted before the identity authentication is taken as an example for illustration. In some embodiments, the file to be encrypted is encrypted after the identity authentication process, and the following takes two examples for specific illustration. In the illustration of the following two specific examples, it is assumed that a file A is a file that is unencrypted and needs to be encrypted, and that the encryption/decryption software is used to perform the user identity authentication and file encryption/decryption is taken as an example for illustration.

[0079] Specific example 1

[0080] In the specific example 1, for the file A, in order to encrypt the file A, an adopted encryption manner is as follows:

[0081] An identity of a user logging in or running the encryption/decryption software is authenticated, and during specific authentication, the identity authentication may be performed by inputting a password, fingerprint information, a facial image, or audio data of the encryption/decryption software registered by the user, or the like.

[0082] After the authentication succeeds, a directory where the file A is located is found through the encryption/decryption software, and the encryption/decryption software is used to encrypt the file A, so as to obtain an encrypted target file A' after the file A is encrypted, and key information a corresponding to the encrypted target file A' is generated. The key information and the encrypted target file A' may be correspondingly stored, and as for a specific storage location, they are locally stored or are stored in a remote server.

[0083] After the file A is encrypted, an original file A may be deleted to prevent the unencrypted original file A from being easily obtained by others and thus affecting the security. A process of deleting the original file A may be performed by the encryption/decryption software or may be manually performed by the user, and preferably, it may be performed by the encryption/decryption software, so as to avoid a situation where the user misses deleting the file, and further improve the security.

[0084] In a situation where the user has not exited current login state in the encryption/decryption software, when it is required to run the encrypted target file A', the encrypted target file A' may be directly clicked to run, and the encryption/decryption software

invokes the key information a corresponding to the file A' after receiving an instruction of clicking to run the encrypted target file A', performs the memory-based decryption on the file A' in the memory by using the key information a, and directly opens or runs the file A on which the memory-based decryption is performed after the memory-based decryption.

[0085] In a situation where the user has exited current login state in the encryption/decryption software, when it is required to run the encrypted target file A', the following are included:

[0086] The user runs the encryption/decryption software, and the encryption/decryption software performs user identity authentication to implement login of the user.

[0087] After the user identity authentication succeeds, the encryption/decryption software obtains an encrypted target file list relevant to the user, where the encrypted target file list includes information of encrypted target files relevant to the user. In a specific implementation, the encrypted target file list represents a relevant encrypted target file through a shortcut icon and so on.

[0088] Then, the user selects to run the encrypted target file A', that is, sends an instruction of running the file A' by clicking the file A' in the encrypted target file list or a shortcut icon thereof.

[0089] The encryption/decryption software obtains the key information a corresponding to the file A' after receiving the instruction, and performs the memory-based decryption on the file A' in the memory by using the key information a. The file on which the memory-based decryption is performed is directly opened and run.

[0090] After the file A is run, the user may perform a relevant operation such as editing processing on the file A. Because the content of the file changes, here, the file on which the editing processing operation is performed is marked as A". After the operation such as editing processing is completed, the user closes the file A"; and after detecting or receiving the closing instruction, the encryption/decryption software encrypts, by using the key information a, the file A" on which the user performs an operation such as editing, stores the encrypted file as the encrypted target file A', and deletes memory data relevant to the file A' in the memory at the same time, so as to ensure that information data relevant to the encrypted

target file A' cannot be easily obtained by people, thereby further ensuring the security of the encrypted target file A'.

[0091] Specific example 2

[0092] In the specific example 2, for the file A, in order to encrypt the file A, an adopted encryption manner is as follows:

[0093] The user directly invokes the encryption/decryption software to encrypt the file A after finding a directory where the file A is located.

[0094] After receiving the instruction, the encryption/decryption software performs authentication on an identity of the user logging in or running the encryption/decryption software, and a specific identity authentication manner may be the same as that in the specific example 1.

[0095] After the identity authentication succeeds, the encryption/decryption software encrypts the file A, so as to obtain an encrypted target file A' after the file A is encrypted, and key information a corresponding to the encrypted target file A' is generated. The key information and the encrypted target file A' are correspondingly stored, and as for a specific storage location, they are locally stored or are stored in a remote server.

[0096] After the file A is encrypted, an original file A is optionally deleted to avoid that the unencrypted original file A is easily obtained by others and thus affecting the security. A process of deleting the original file A may be performed by the encryption/decryption software or may be manually performed by the user, and preferably, it is performed by the encryption/decryption software, so as to avoid a situation where the user misses deleting the file, and further improve the security.

[0097] After the file A is encrypted, and when the user needs to run the encrypted target file A', the following are included:

[0098] The user runs the encryption/decryption software, and the encryption/decryption software performs user identity authentication to implement login of the user.

[0099] After the user identity authentication succeeds, the encryption/decryption software obtains an encrypted target file list relevant to the user, where the encrypted target file list includes information of encrypted target files relevant to the user. In a specific implementation, the encrypted target file list is represented through a shortcut icon and so on.

[00100] Then, the user selects to run the encrypted target file A', that is, sends an instruction of running the file A' by clicking the file A' in the encrypted target file list or a shortcut icon thereof.

[0100] The encryption/decryption software obtains the key information a corresponding to the file A' after receiving the instruction, and performs the memory-based decryption on the file A' in the memory by using the key information a. The file on which the memory-based decryption is performed is directly opened and run.

[0101] After the file A is run, the user may perform a relevant operation such as editing processing on the file A. Because the content of the file changes, here, the file on which the editing processing operation is performed is marked as A". After the operation such as editing processing is completed, the user closes the file A"; and after detecting or receiving the closing instruction, the encryption/decryption software encrypts, by using the key information a, the file A" on which the user performs an operation such as editing, stores the encrypted file as the encrypted target file A', and deletes memory data relevant to the file A' in the memory at the same time, so as to ensure that information data relevant to the encrypted target file A' cannot be easily obtained by people, thereby further ensuring the security of the encrypted target file A'.

[0102] In this embodiment, other technical features are the same as those in Embodiment 2, which are not elaborated herein.

[0103] In addition, according to the solutions in the embodiments of the file encryption and running method of the present invention, when the encrypted target file needs to be opened, the corresponding key information is directly invoked in the memory to perform decryption, and the user does not need to manually input the password of the encrypted target file. For example, when the file is opened through the encryption/decryption software, the user only needs to remember a password of logging in the encryption/decryption

software, which avoids a situation where the file cannot be decrypted and run because the password of the encrypted target file is forgotten, thereby not only improving the efficiency of running the encrypted file but also improving the convenience of running the encrypted file.

[0104] According to the file encryption and running method of the present invention, the present invention further provides a file encryption and running system. The following illustrates embodiments of the file encryption and running system of the present invention.

[0105] FIG. 5 shows a block diagram of Embodiment 1 of a computer system according to some embodiments of the present invention.

[0106] As shown in FIG. 5, the file encryption and running system in Embodiment 1 includes: a running instruction receiving unit 501, configured to receive a file running instruction; and a file running unit 502, configured to invoke an encrypted target file according to the running instruction, perform memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed.

[0107] According to the solution in this embodiment, when it is required to run the encrypted target file, the key information corresponding to the encrypted target file is obtained, the memory-based decryption is performed on the encrypted target file in a memory by using the key information, and the encrypted target file is directly run after the memory-based decryption is completed. In this file running manner, the file can be opened and run without manually inputting a password of the encrypted target file and manually decrypting the file, thereby improving the efficiency of running the encrypted file. In another aspect, the encrypted target file is decrypted in the memory by using the key information, so that the decrypted file is stored in the memory without generating a permanent file, and therefore, it cannot be stolen by people, thereby further improving the security of running the encrypted file.

[0108] As shown in FIG. 5, the file encryption and running system in this embodiment optionally includes: a memory clear unit 503, configured to clear memory data corresponding

to the encrypted target file after running when an instruction of closing the encrypted target file after running is received.

[0109] Therefore, the encrypted target file that is run before does not leave relevant data information in the memory after the running encrypted target file is closed, so that information data relevant to the encrypted target file cannot be easily obtained by people, which further ensures the security of the encrypted target file.

[0110] When clearing the memory data, the memory clear unit 503, after receiving the instruction of closing the encrypted target file after running, may give a prompt about whether to clear the memory data, and clear the memory data corresponding to the encrypted target file after running when receiving the instruction of clearing the memory data, or may automatically and directly clear the memory data corresponding to the encrypted target file after running when receiving the instruction of closing the encrypted target file after running, so as to enhance the security.

[0111] In addition, when receiving the instruction of closing the encrypted target file after running, the memory clear unit 503 may further perform encryption by directly invoking key information corresponding to the encrypted target file, so that the encrypted target file after running does not need to be manually encrypted, thereby further improving the efficiency of running the encrypted file.

[0112] FIG. 6 shows a block diagram of Embodiment 2 of a computer system according to some embodiments of the present invention.

[0113] As shown in FIG. 6, the difference from Embodiment 1 mainly lies in that the file encryption and running system in Embodiment 2 further includes: an encryption instruction running unit 601, configured to receive a file encryption instruction, encrypt a file to be encrypted to obtain the encrypted target file, and generate the key information corresponding to the encrypted target file; and a storage unit 602, configured to store the key information and the corresponding encrypted target file.

[0114] According to the solution in this embodiment, when the file is encrypted, the key information corresponding to the encrypted target file is generated, and the key information and the encrypted target file are correspondingly stored, so that when it is required to run the

encrypted target file, the corresponding key information thereof is directly obtained, and the encrypted target file is decrypted in a memory by using the key information. Therefore, the file can be opened and run without manually inputting a password of the encrypted target file and manually decrypting the file, thereby improving the efficiency of running the encrypted file. In another aspect, the encrypted target file is decrypted in the memory by using the key information, so that the decrypted file is stored in the memory without generating a permanent file, and therefore, it cannot be thieved by people, thereby further improving the security of running the encrypted file.

[0115] When the key information and the encrypted target file are correspondingly stored, different settings may be made according to different specific requirements.

[0116] In some embodiments, the storage unit 602 is set locally, and in this case, the key information and the encrypted target file are stored in the local storage unit 602 at the same time.

[0117] In some other embodiments, the storage unit 602 is set in a remote server, and in this case, the key information and the encrypted target file are stored in the storage unit 602 set in the remote server at the same time.

[0118] In some further embodiments, the storage unit 602 is set as multiple small storage units. For example, the storage unit 602 is set as two small storage units: a first storage unit (not shown) and a second storage unit (not shown), where the first storage unit is locally set, and the second storage unit is set in a remote server. In this case, one of the key information and the encrypted target file is stored in the first storage unit, and the other is stored in the second storage unit, and different settings may be made according to different specific requirements.

[0119] In some further embodiments, in the foregoing first two embodiments, when the key information and the encrypted target file both are locally stored or stored in the remote server, the key information and the encrypted target file are combined into one file and stored, or the key information and the encrypted target file are stored as two separate files, so as to enhance the security, as long as a corresponding key relationship can be obtained based on

the corresponding storage relationship to decrypt the encrypted target file, when the encrypted target file needs to be opened.

[0120] In addition, after obtaining the encrypted target file, the encryption instruction running unit 601, optionally, further deletes the file to be encrypted. Therefore, an original file (the file to be encrypted) does not leave relevant data information after the encrypted target file is obtained, so that information data relevant to the encrypted target file cannot be easily obtained by people, which further ensures the security of the encrypted target file.

[0121] Other technical features of the file encryption and running system in Embodiment 2 are the same as those in the file encryption and running system in Embodiment 1, which are not elaborated herein.

[0122] FIG. 7 shows a block diagram of Embodiment 3 of a file encryption system according to some embodiments of the present invention.

[0123] As shown in FIG. 7, the difference from Embodiment 1 mainly lies in that the file encryption and running system in Embodiment 3 further includes: an identity authentication unit 701, configured to receive an identity authentication instruction, and perform authentication on a login identity; and a file list obtaining unit 702, configured to obtain an encrypted target file list corresponding to the authenticated identity after the identity authentication unit 701 succeeds in the authentication.

[0124] According to the solution in Embodiment 3, after the user identity authentication succeeds, a user that currently logs in or a user that needs to run an encrypted target file in the encrypted target file list is trusted, so that when it is required to run the encrypted target file, the corresponding key information thereof is directly obtained, and the encrypted target file is decrypted in a memory by using the key information. Therefore, the file can be opened and run without manually inputting a password of the encrypted target file and manually decrypting the file, thereby improving the efficiency of running the encrypted file. In another aspect, the encrypted target file is decrypted in the memory by using the key information, so that the decrypted file is stored in the memory without generating a permanent file, and therefore, it cannot be thieved by people, thereby further improving the security of running the encrypted file.

[0125] When the user identity is authenticated, various possible manners may be adopted, for example, the identity authentication is performed according to information such as a numeric password, a facial image, fingerprint information, or audio data of a user, and a specific identity authentication manner is not elaborated herein.

[0126] Other technical features of the file encryption and running system in Embodiment 3 are the same as those in the file encryption and running system in Embodiment 1, which are not elaborated herein.

[0127] FIG. 8 shows a block diagram of Embodiment 4 of a computer system according to some embodiments of the present invention.

[0128] As shown in FIG. 8, the difference from Embodiment 2 mainly lies in that the file encryption and running system in Embodiment 4 further includes: an identity authentication unit 701, configured to receive an identity authentication instruction, and perform authentication on a login identity; and a file list obtaining unit 702, configured to obtain an encrypted target file list corresponding to the authenticated identity after the identity authentication unit 701 succeeds in the authentication.

[0129] According to the solution in Embodiment 4, when the file is encrypted, the key information corresponding to the encrypted target file is generated, and the key information and the encrypted target file are correspondingly stored, so that when it is required to run the encrypted target file, the user identity is authenticated, and a user that currently logs in or a user that needs to run an encrypted target file in the encrypted target file list is trusted after the authentication succeeds. Therefore, when it is required to run the encrypted target file, the corresponding key information thereof is directly obtained, and the encrypted target file is decrypted in a memory by using the key information. Therefore, the file can be opened and run without manually inputting a password of the encrypted target file and manually decrypting the file, thereby improving the efficiency of running the encrypted file. In another aspect, the encrypted target file is decrypted in the memory by using the key information, so that the decrypted file is stored in the memory without generating a permanent file, and therefore, it cannot be stolen by people, thereby further improving the security of running the encrypted file.

[0130] When the user identity is authenticated, various possible manners may be adopted. For example, the identity authentication is performed according to information such as a numeric password, a facial image, fingerprint information, or audio data of a user, and a specific identity authentication manner is not elaborated herein.

[0131] Other technical features of the file encryption and running system in Embodiment 4 are the same as those in the file encryption and running system in Embodiment 2, which are not elaborated herein.

[0132] According to the file encryption and running system in each embodiment of the present invention, a specific file encryption and running manner may be the same as that in the file encryption and running method of the present invention, which is not elaborated herein.

[0133] Fig. 9 is a block diagram illustrating a device 900 in accordance with some embodiments of the present invention. The device 900 typically includes one or more processing units (CPU's) 902 for executing modules, programs and/or instructions stored in memory 912 and thereby performing processing operations; one or more network or other communications interfaces 910; memory 912; and one or more communication buses 914 for interconnecting these components. The communication buses 914 optionally include circuitry (sometimes called a chipset) that interconnects and controls communications between system components. The device 900 optionally includes a user interface 904 comprising a display device 906 and one or more input device(s) (e.g., keyboard, mouse, touch-sensitive surface) 908. In some embodiments, an input device 908 is integrated with the display device 906. For example, a touch screen includes a touch-sensitive surface integrated with the display device 906. Memory 912 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM or other random access solid state memory devices; and may include non-volatile memory, such as one or more magnetic disk storage devices, optical disk storage devices, flash memory devices, or other non-volatile solid state storage devices. Memory 912 may optionally include one or more storage devices remotely located from the CPU(s) 902. Memory 912, or alternately the non-volatile memory device(s) within memory 912, comprises a non-transitory computer readable storage medium.

In some embodiments, memory 912, or the computer readable storage medium of memory 912 stores the following programs, modules and data structures, or a subset thereof:

[0134] an operating system 916 that includes procedures for handling various basic system services and for performing hardware dependent tasks;

[0135] a network communication module 918 that is used for connecting the device 900 to other computers via the one or more communication network interfaces 910 (wired or wireless) and one or more communication networks, such as the Internet, other wide area networks, local area networks, metropolitan area networks, and so on;

[0136] a running instruction receiving unit 501, configured to receive a file running instruction;

[0137] a file running unit 502, configured to invoke an encrypted target file according to the running instruction, perform memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed;

[0138] a memory clear unit 503, configured to clear memory data corresponding to the encrypted target file after running when an instruction of closing the encrypted target file after running is received;

[0139] an encryption instruction running unit 601, configured to receive a file encryption instruction, encrypt a file to be encrypted to obtain the encrypted target file, and generate the key information corresponding to the encrypted target file;

[0140] a storage unit 602, configured to store the key information and the corresponding encrypted target file;

[0141] an identity authentication unit 701, configured to receive an identity authentication instruction, and perform authentication on a login identity;

[0142] a file list obtaining unit 702, configured to obtain an encrypted target file list corresponding to the authenticated identity after the identity authentication unit 701 succeeds in the authentication;

[0143] files 920, among which include encrypted files 922; and

[0144] key information 924 corresponding to encrypted files 922.

[0145] The encryption instruction running unit 602 encrypts a (unencrypted) file 920 to obtain an encrypted file 922 and generate the corresponding key information 924. The file running unit 502 invokes an encrypted file 922 according to a running instruction, performs memory-based decryption on the encrypted file 922 according to key information 924 corresponding to the encrypted file 922, and runs the encrypted file 922 on which the memory-based decryption is performed.

[0146] Each of the above identified elements may be stored in one or more of the previously mentioned memory devices, and corresponds to a set of instructions for performing a function described above. The above identified modules, units or programs (i.e., sets of instructions) need not be implemented as separate software programs, procedures, units or modules, and thus various subsets of these modules may be combined or otherwise re-arranged in various embodiments. In some embodiments, memory 912 may store a subset of the modules and data structures identified above. Furthermore, memory 912 may store additional modules and data structures not described above.

[0147] Although Fig. 9 shows a "device," Fig. 9 is intended more as functional description of the various features which may be present in a set of servers than as a structural schematic of the embodiments described herein. In practice, and as recognized by those of ordinary skill in the art, items shown separately could be combined and some items could be separated.

[0148] The foregoing embodiments only show several implementation manners of the present invention and are described in details, but they should not be construed as a limit to the scope of the patent of the present invention. It should be noted that, persons of ordinary skill in the art may make various changes and improvements without departing from the ideas of the present invention, which shall fall within the protection scope of the present invention. Therefore, the protection scope of the patent of the present invention shall be subject to that of the claims.

[0149] While particular embodiments are described above, it will be understood it is not intended to limit the invention to these particular embodiments. On the contrary, the

invention includes alternatives, modifications and equivalents that are within the spirit and scope of the appended claims. Numerous specific details are set forth in order to provide a thorough understanding of the subject matter presented herein. But it will be apparent to one of ordinary skill in the art that the subject matter may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the embodiments.

[0150] Although the terms first, second, etc. may be used herein to describe various elements, these elements should not be limited by these terms. These terms are only used to distinguish one element from another. For example, first ranking criteria could be termed second ranking criteria, and, similarly, second ranking criteria could be termed first ranking criteria, without departing from the scope of the present invention. First ranking criteria and second ranking criteria are both ranking criteria, but they are not the same ranking criteria.

[0151] The terminology used in the description of the invention herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used in the description of the invention and the appended claims, the singular forms "a," "an," and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will also be understood that the term "and/or" as used herein refers to and encompasses any and all possible combinations of one or more of the associated listed items. It will be further understood that the terms "includes," "including," "comprises," and/or "comprising," when used in this specification, specify the presence of stated features, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, operations, elements, components, and/or groups thereof.

[0152] As used herein, the term "if" may be construed to mean "when" or "upon" or "in response to determining" or "in accordance with a determination" or "in response to detecting," that a stated condition precedent is true, depending on the context. Similarly, the phrase "if it is determined [that a stated condition precedent is true]" or "if [a stated condition precedent is true]" or "when [a stated condition precedent is true]" may be construed to mean "upon determining" or "in response to determining" or "in accordance with a determination" or "upon detecting" or "in response to detecting" that the stated condition precedent is true, depending on the context.

[0153] Although some of the various drawings illustrate a number of logical stages in a particular order, stages that are not order dependent may be reordered and other stages may be combined or broken out. While some reordering or other groupings are specifically mentioned, others will be obvious to those of ordinary skill in the art and so do not present an exhaustive list of alternatives. Moreover, it should be recognized that the stages could be implemented in hardware, firmware, software or any combination thereof.

[0154] The foregoing description, for purpose of explanation, has been described with reference to specific implementations. However, the illustrative discussions above are not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The implementations were chosen and described in order to best explain principles of the invention and its practical applications, to thereby enable others skilled in the art to best utilize the invention and various implementations with various modifications as are suited to the particular use contemplated. Implementations include alternatives, modifications and equivalents that are within the spirit and scope of the appended claims. Numerous specific details are set forth in order to provide a thorough understanding of the subject matter presented herein. But it will be apparent to one of ordinary skill in the art that the subject matter may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the implementations.

WHAT IS CLAIMED IS:

1. A computer-implemented method for running an encrypted file, comprising:

at a computer having one or more processors and memory for storing programs to be executed by the one or more processors:

receiving a file running instruction;

invoking an encrypted target file according to the file running instruction, and performing memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file; and

running the encrypted target file on which the memory-based decryption is performed.

2. The method according to claim 1, before the step of receiving a file running instruction, further comprising:

receiving a file encryption instruction, encrypting a file to be encrypted to obtain the encrypted target file, generating the key information corresponding to the encrypted target file, and storing the key information and the corresponding encrypted target file.

3. The method according to claim 2, after the step of obtaining the encrypted target file, further comprising: deleting the file to be encrypted.

4. The method according to claim 2, wherein:

the key information and the encrypted targeted file are locally stored or stored in a server, and the key information and the encrypted target file are combined and stored into a unified file.

5. The method according to claim 2, wherein:

the key information and the encrypted targeted file are locally stored or stored in a server, and the key information and the encrypted target file are respectively stored as separate files.

6. The method according to claim 2, wherein:

the key information is locally stored and the encrypted targeted file is stored in a server.

7. The method according to claim 2, wherein:

the key information is stored in a server and the encrypted targeted file is locally stored.

8. The method according to claim 1, before the step of receiving a file running instruction, further comprising:

receiving an identity authentication instruction, and obtaining an encrypted target file list corresponding to the authenticated identity after the identity authentication succeeds.

9. The method according to claim 8, wherein the identity authentication is performed through one of a numeric password, a facial image, fingerprint information, or audio data of a user.

10. The method according to claim 1, further comprising:

automatically and directly clearing memory data corresponding to the encrypted target file after running when an instruction of closing the encrypted target file after running is received.

11. The method according to claim 10, when the instruction of closing the encrypted target file after running is received, further comprising: invoking the key information to encrypt the encrypted target file after running.

12. The method according to claim 1, further comprising:

when an instruction of closing the encrypted target file after running is received, giving a prompt about whether to clear memory data, and clearing memory data corresponding to the encrypted target file after running when an instruction of clearing the memory data is received.

13. The method according to claim 12, when the instruction of closing the encrypted target file after running is received, further comprising: invoking the key information to encrypt the encrypted target file after running.

14. A computer system for running an encrypted file, comprising:

one or more processors;

memory; and

one or more program units stored in the memory and to be executed by the one or

more processors, the one or more program units including:

a running instruction receiving unit, configured to receive a file running instruction; and

a file running unit, configured to invoke an encrypted target file according to the running instruction, perform memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed.

15. The computer system according to claim 14, wherein the one or more program units further include:

an encryption instruction running unit, configured to receive a file encryption instruction, encrypt a file to be encrypted to obtain the encrypted target file, and generate the key information corresponding to the encrypted target file; and

a storage unit, configured to store the key information and the corresponding encrypted target file.

16. The computer system according to claim 15, wherein:

the encryption instruction running unit is further configured to: after obtaining the encrypted target file, delete the file to be encrypted.

17. The computer system according to claim 15, wherein:

the storage unit comprises a first storage unit set locally and a second storage unit set in a server, and the key information is stored in the first storage unit and the encrypted file information is stored in the second storage unit, or the key information is stored in the second storage unit and the encrypted file information is stored in the first storage unit.

18. The computer system according to claim 15, further comprising:

an identity authentication unit, configured to receive an identity authentication instruction, and perform authentication on a login identity; and

a file list obtaining unit, configured to obtain an encrypted target file list corresponding to the authenticated identity after the identity authentication unit succeeds in the authentication.

19. A computer readable storage medium storing one or more programs, the one or more programs comprising instruction which, when executed by a device, cause the device to:

receive a file running instruction;

invoke an encrypted target file according to the file running instruction, and perform memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file; and

run the encrypted target file on which the memory-based decryption is performed.

20. The computer readable storage medium of claim 19, including instructions which cause the device to:

before receiving a file running instruction, receive a file encryption instruction, encrypt a file to be encrypted to obtain the encrypted target file, generate the key information corresponding to the encrypted target file, and store the key information and the corresponding encrypted target file.

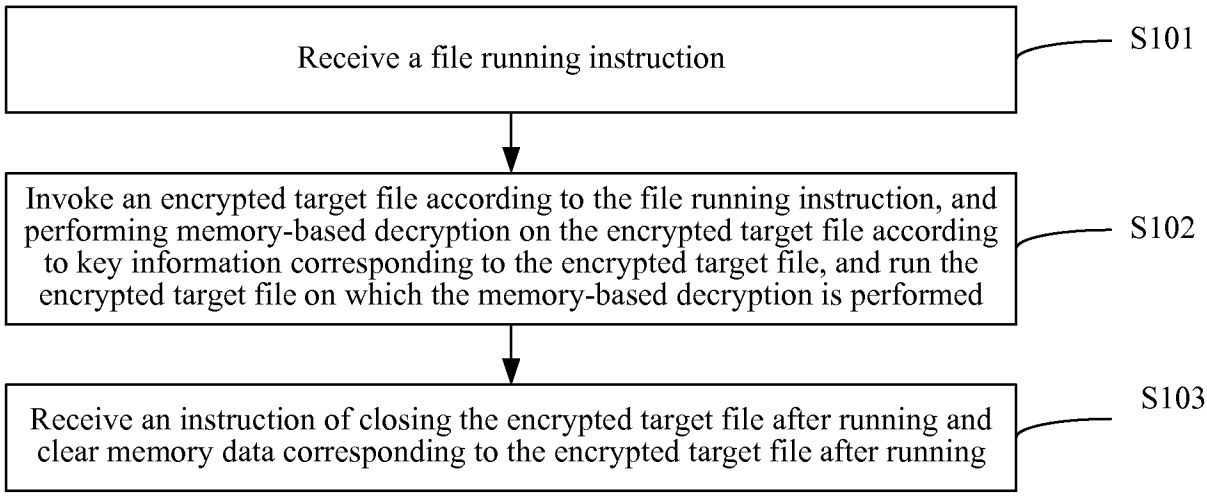

Receive a file running instruction
S101
Invoke an encrypted target file according to the file running instruction, and performing memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed
S102
Receive an instruction of closing the encrypted target file after running and clear memory data corresponding to the encrypted target file after running
S103

FIG. 1

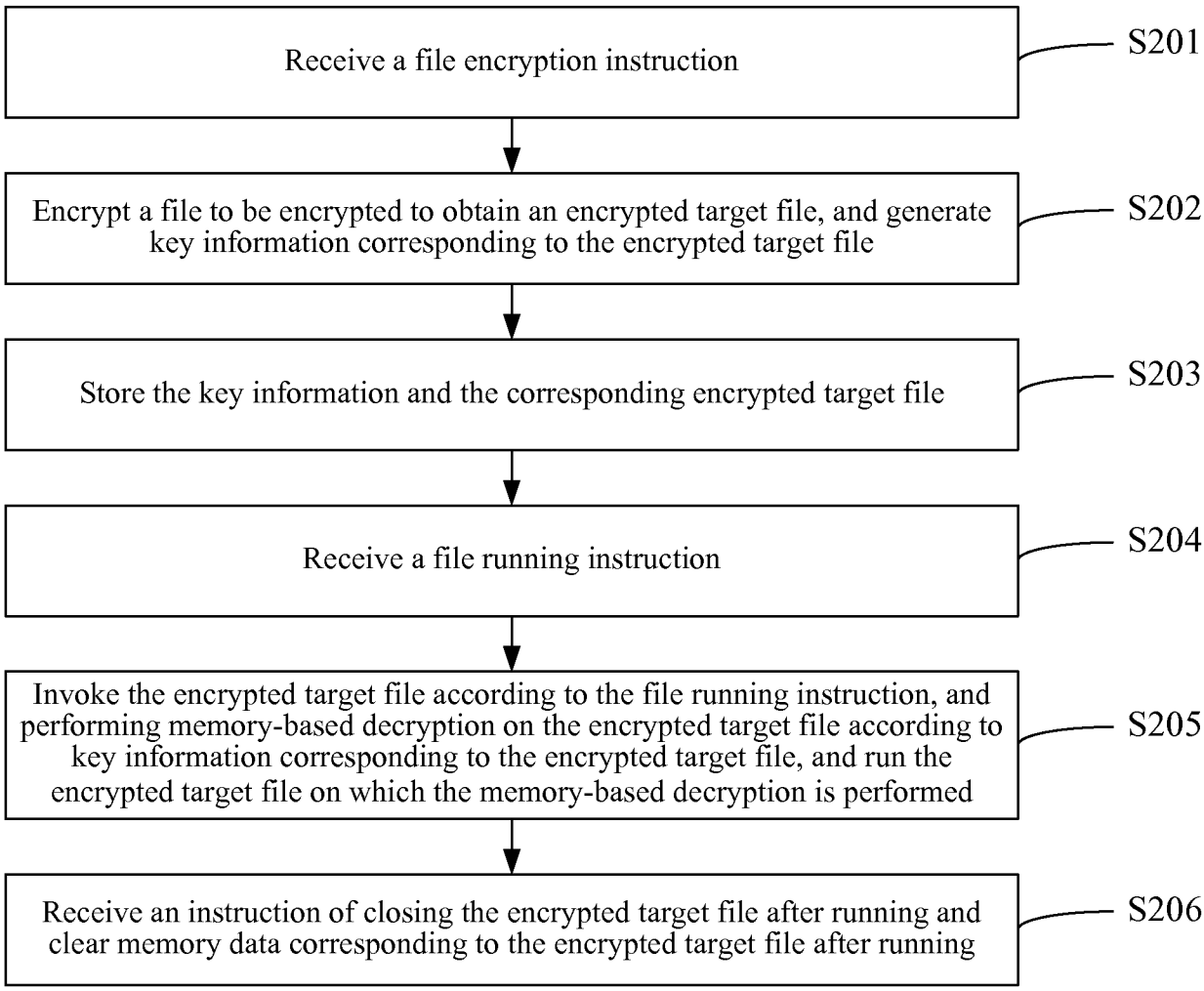

Receive a file encryption instruction
S201
Encrypt a file to be encrypted to obtain an encrypted target file, and generate key information corresponding to the encrypted target file
S202
Store the key information and the corresponding encrypted target file
S203
Receive a file running instruction
S204
Invoke the encrypted target file according to the file running instruction, and performing memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed
S205
Receive an instruction of closing the encrypted target file after running and clear memory data corresponding to the encrypted target file after running
S206

FIG. 2

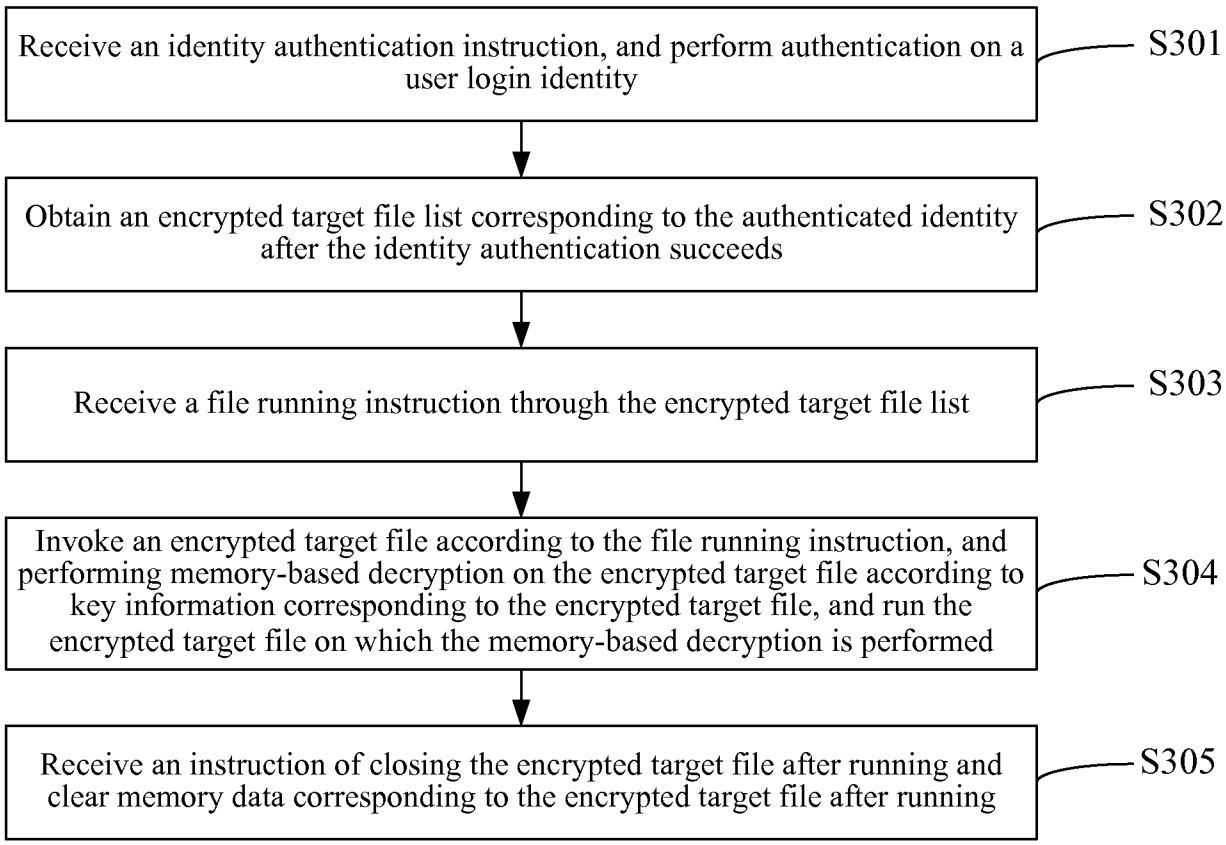

Receive an identity authentication instruction, and perform authentication on a user login identity
S301
Obtain an encrypted target file list corresponding to the authenticated identity after the identity authentication succeeds
S302
Receive a file running instruction through the encrypted target file list
S303
Invoke an encrypted target file according to the file running instruction, and performing memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed
S304
Receive an instruction of closing the encrypted target file after running and clear memory data corresponding to the encrypted target file after running
S305

FIG. 3

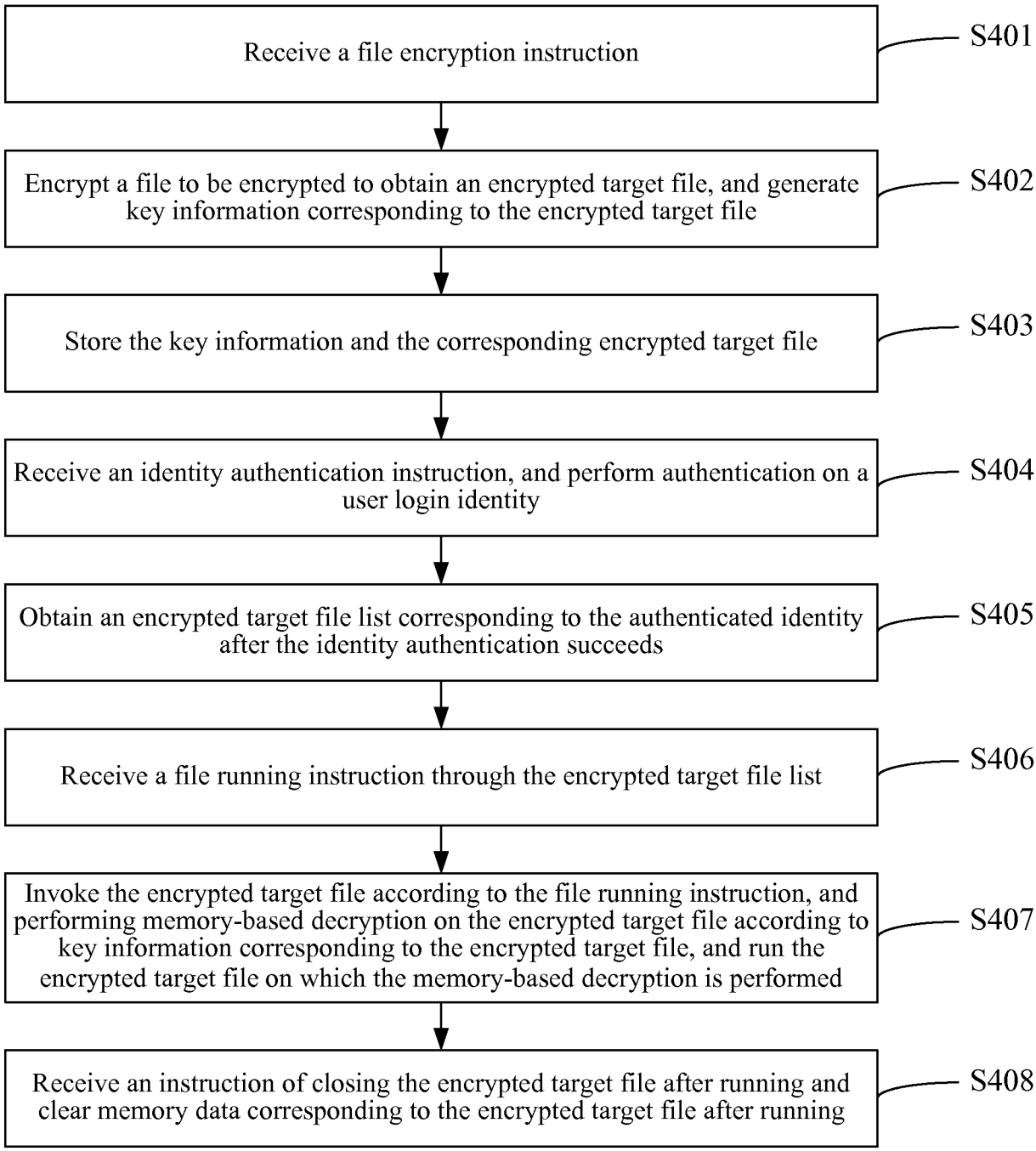

Receive a file encryption instruction
S401
Encrypt a file to be encrypted to obtain an encrypted target file, and generate key information corresponding to the encrypted target file
S402
Store the key information and the corresponding encrypted target file
S403
Receive an identity authentication instruction, and perform authentication on a user login identity
S404
Obtain an encrypted target file list corresponding to the authenticated identity after the identity authentication succeeds
S405
Receive a file running instruction through the encrypted target file list
S406
Invoke the encrypted target file according to the file running instruction, and performing memory-based decryption on the encrypted target file according to key information corresponding to the encrypted target file, and run the encrypted target file on which the memory-based decryption is performed
S407
Receive an instruction of closing the encrypted target file after running and clear memory data corresponding to the encrypted target file after running
S408

FIG. 4

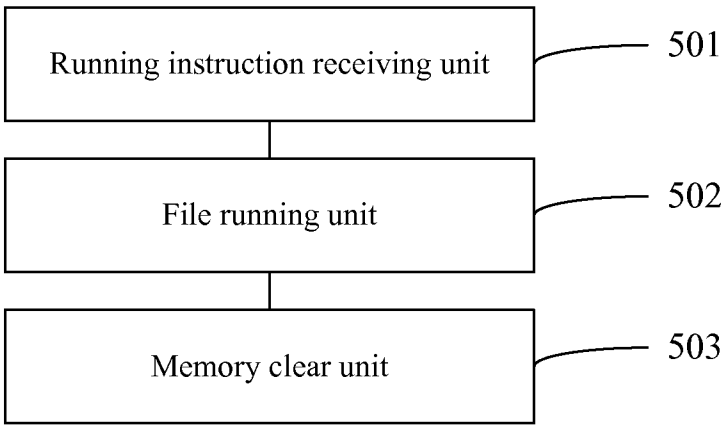

Running instruction receiving unit
501
File running unit
502
Memory clear unit
503

FIG. 5

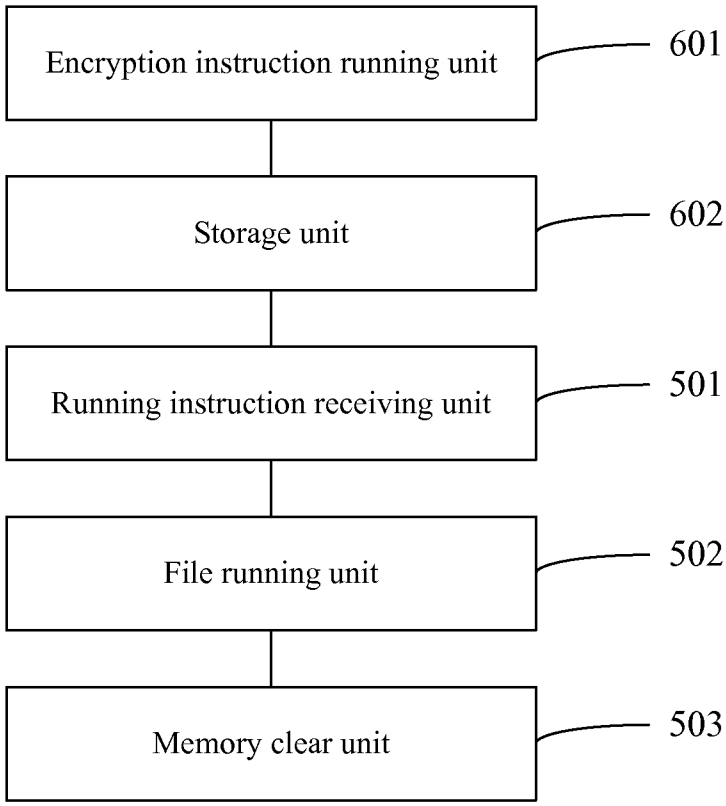

Encryption instruction running unit
601
Storage unit
602
Running instruction receiving unit
501
File running unit
502
Memory clear unit
503

FIG. 6

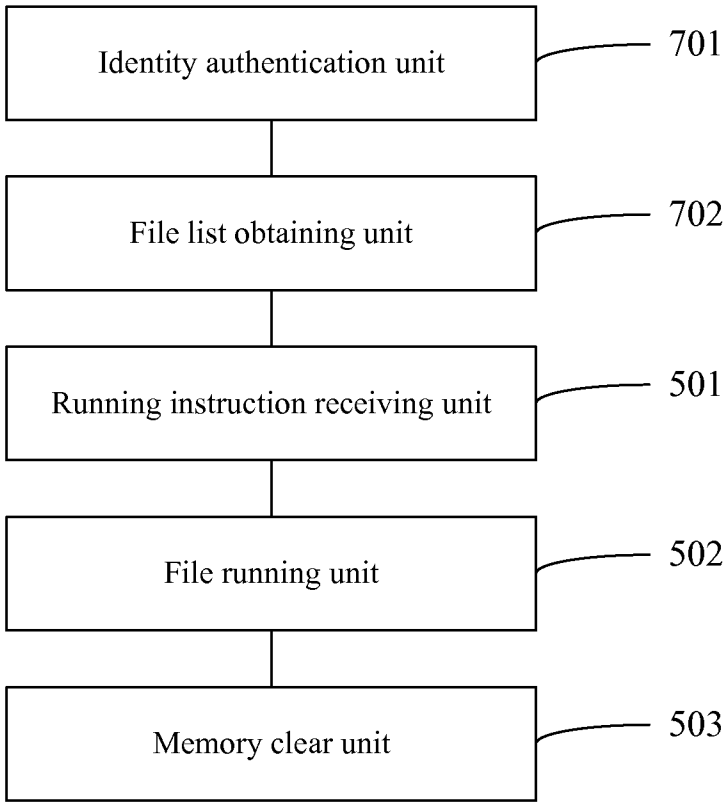

Identity authentication unit
701
File list obtaining unit
702
Running instruction receiving unit
501
File running unit
502
Memory clear unit
503

FIG. 7

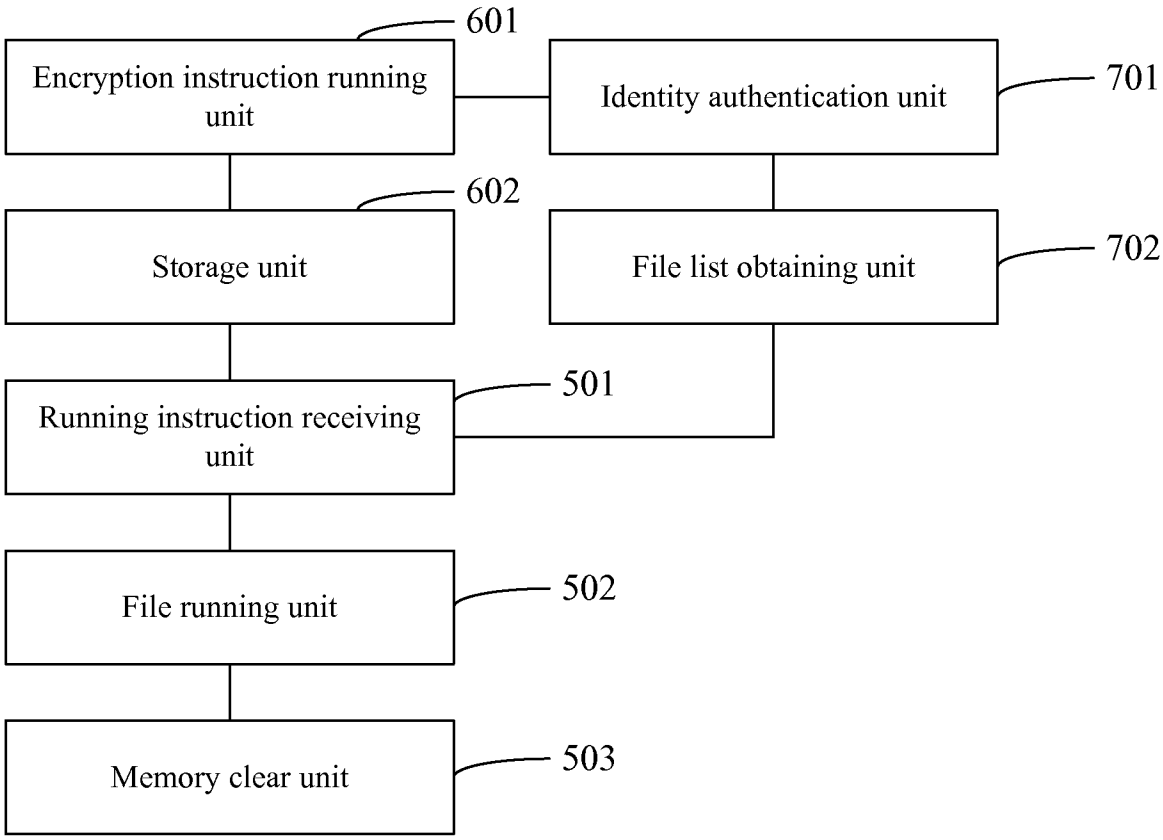

601
Encryption instruction running unit
Identity authentication unit
701
602
Storage unit
File list obtaining unit
702
501
Running instruction receiving unit
File running unit
502
Memory clear unit
503

FIG. 8

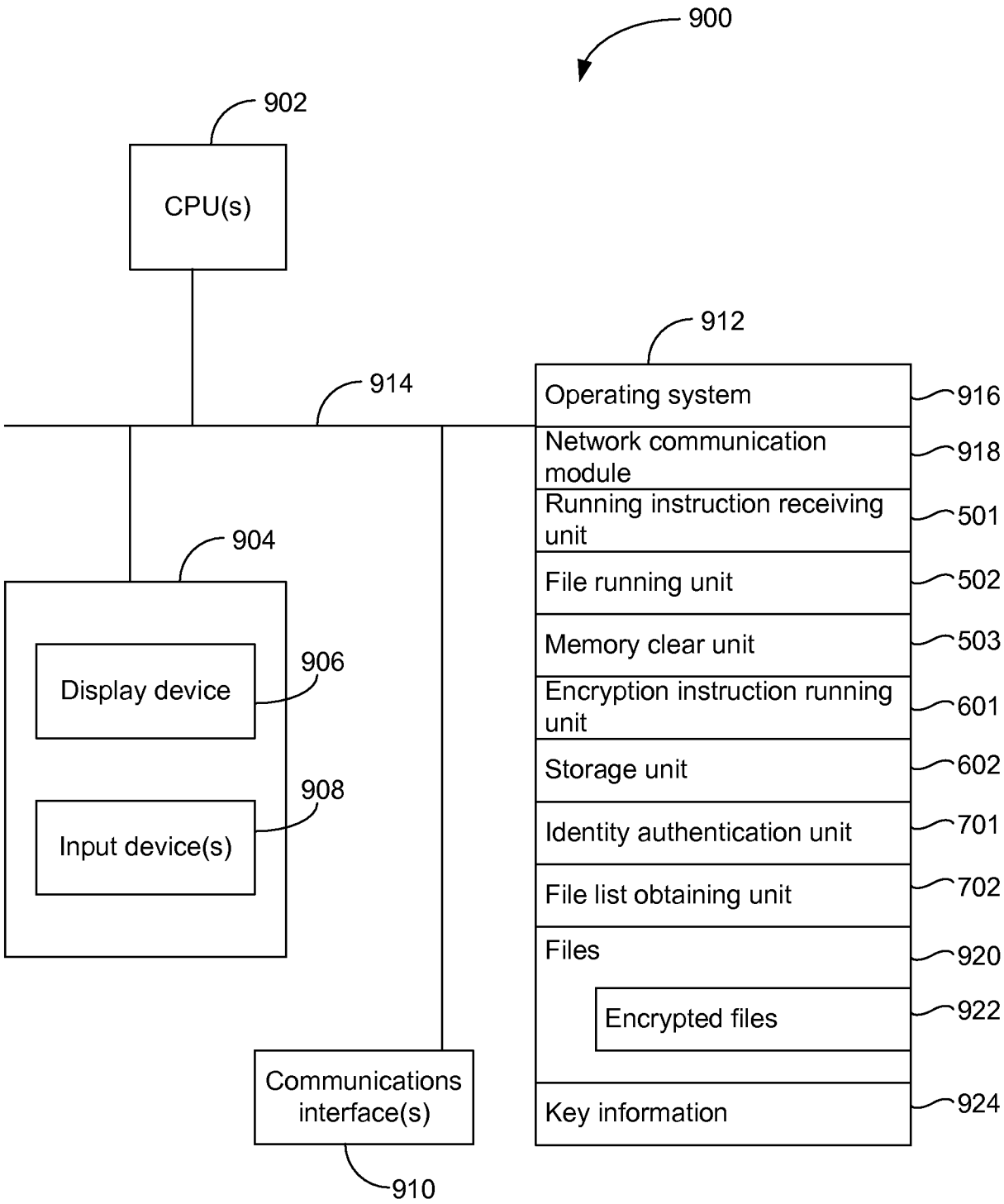

900
902
CPU(s)
912
914
Operating system
916
Network communication module
918
Running instruction receiving unit
501
904
File running unit
502
Memory clear unit
503
Display device
906
Encryption instruction running unit
601
Storage unit
602
908
Input device(s)
Identity authentication unit
701
File list obtaining unit
702
Files
920
Encrypted files
922
Communications interface(s)
Key information
924
910

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/079589

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00 (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: G06F 9/-, G06F 21/-

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)

CNABS,DWPI,VEN,CNKI: encrypt+, decrypt+, key, auto+, automatic, delete, origin, original, file?, memory, run, security, manual+, password?, authentication, efficiency, local, remote, server, enhance

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 102819702 A (TENCENT TECHNOLOGY SHENZHEN CO LTD) 12 December 2012 (12.12.2012) claims 1-22, description paragraph [0021] to paragraph [0142]	1-20
X	WO 2007/014790 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION)	1-2,4-15,17-20
Y	08 February 2007 (08.02.2007) abstract, description page 15 line 1 to page 17 line 2, page 8 line 15 to page 10 line 8 and figure 7	3,16
Y	CN 101008974 A (BEIJING FEITIAN CHENGXIN SCITECH CO LTD) 01 August 2007 (01.08. 2007) description page 5 line 15 to line 22	3,16

☐ 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 another 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
16 September 2013 (16.09.2013)	**24 Oct. 2013 (24.10.2013)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer Liu, Jia Telephone No. (86-10)62411655

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/079589

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102819702 A	12.12.2012	None	
WO 2007/014790 A1	08.02.2007	KR100968190B1	07.07.2010
		JP4755689B2	24.08.2011
		EP1908249A1	09.04.2008
		CN101228770A	23.07.2008
		TW200719651A	16.05.2007
		CN101228770B	14.12.2011
		US2010281254A1	04.11.2010
		EP1908249B1	15.08.2012
		JP2009503661A	29.01.2009
		KR20080025169A	19.03.2008
CN 101008974 A	01.08 2007	CN100446024C	24.12.2008