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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 February 2015 (05.02.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/014308 A1

(51) International Patent Classification:
H04L 1/00 (2006.01)

(21) International Application Number:
PCT/CN2014/083515

(22) International Filing Date:
1 August 2014 (01.08.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201310334412.4 2 August 2013 (02.08.2013) CN

(71) Applicant: **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN).

(72) Inventor: **GUAN, Shengyu**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN).

(74) Agent: **ADVANCE CHINA IP LAW OFFICE**; Room 3901, No. 85 Huacheng Avenue, Tianhe District, Guangzhou, Guangdong 510623 (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, IR, 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, SA, 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))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: A METHOD AND A DEVICE FOR DATA PROCESSING

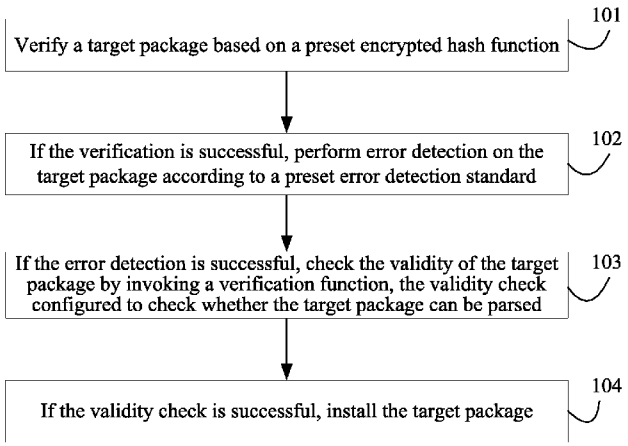

Figure 1

(57) **Abstract**: A method and a device are provided for solving the problem of low success rates of local Android application package (APK) installations. The method includes: verifying a stored target package based on a preset encrypted hash function; if said verification is successful, performing error detection on said target package according to a preset error detection standard; if said error detection is successful, checking the validity of said target package by invoking a verification function, said validity check being configured to check whether said target package can be parsed; if said validity check is successful, installing said target package.

WO 2015/014308 A1

A METHOD AND A DEVICE FOR DATA PROCESSING

CROSS-REFERENCE TO RELATED APPLICATIONS

[001] This application claims priority to Chinese Patent Application No. 201310334412.4, filed on August 2, 2013, which is hereby incorporated by reference in its entirety.

FIELD

[002] The present disclosure relates to the field of the Internet technologies, particularly to a method and a device for data processing.

BACKGROUND

[003] With the existing art, before application can be installed on a terminal running on an Android™ system, the Android application package (APK) needs to be run on the terminal. A user can download APKs by using a large number of APK download links provided on existing websites. However, due to an original data error or network transmission error that may occur during APK download, the downloaded APK may not be the APK requested by the user and consequently fails to be installed locally.

[004] Generally, for the sake of commercial profits, operators add downlinks to APKs, Such a practice is called download hijack. Download hijack often causes errors in downloaded file streams, namely, original data errors. For example, the downloaded APK may be a download software APK, instead of the game APK requested by the user. Currently, the Message Digest Algorithm 5 (MD5) is configured to check whether an APK downloaded by a user is the APK requested by the user. In addition, an APK is partitioned into multiple sub-packages according to the specified data size for convenient transmission on a network. This gives rise to the problem that some of these sub-packages may get lost during the transmission. In such as case, the APK received by the terminal is incomplete. An APK is a compressed file in the *.zip format. Therefore, currently, the Cyclic Redundancy Check (CRC) is configured to check whether any part of a user-downloaded APK is lost.

[005] Even if the APK downloaded by a user is complete and also the APK requested by the user, parsing of the APK may fail due to a system problem, leading to an APK installation failure. As a result, the success rate of local APK installations is low.

SUMMARY

[006] A method and a device for data processing provided by the present disclosure, capable of solving the problem of low success rates of local APK installations.

[007] In one aspect, the present disclosure provides a method for data processing implemented in a device including a processor. The method includes: verifying a stored target package based on a

preset encrypted hash function; if said verification is successful, performing error detection on said target package according to a preset error detection standard; if said error detection is successful, checking the validity of said target package by invoking a verification function, said validity check being configured to check whether said target package can be parsed; if said validity check is successful, installing said target package.

[008] In another aspect, the present disclosure further provides a device for data processing. The device includes a hardware processor and a non-transitory storage medium. The non-transitory storage medium is configured to store units including: a verification unit, an error detection unit, a validity check unit, and an installation unit. The verification unit is configured to verify a target package stored in the storage unit based on a preset encrypted hash function. The error detection unit is configured to, if the verification performed by said verification unit is successful, perform error detection on said target package based on a preset error detection standard. The validity check unit is configured to, if the detection performed by said error detection unit is successful, perform validity check on said target package by invoking a verification function, said validity check being configured to check whether said target package can be parsed. The installation unit is configured to, if the check performed by said validity check unit is successful, install said target package.

[009] The method and device provided by the present disclosure for data processing may be configured to verify a stored target package based on a preset encrypted hash function, said target package being a package sent by a network-side server according to a user request; if said verification is successful, perform error detection on said target package according to a preset error detection standard; if said error detection is successful, perform validity check on said target package by invoking a verification function, said validity check being configured to check whether said target package can be parsed; if said validity check is successful, install said target package. Verification of a stored target package based on a preset encrypted hash function can ensure that the downloaded target package is the requested package, namely, ensuring that the target package is unique. Error detection on said target package according to a preset error detection standard can ensure that the target package is integral. Validity check on said target package by invoking a verification function can ensure that the target package is valid. The existing art only checks either the integrity or the uniqueness of the target package. By checking the uniqueness, integrity, and validity of target packages, the present disclosure can improve the check efficiency, capable of eliminating, by a larger proportion compared with the existing art, the target packages that cannot be installed. If the target package passes the above-mentioned three checks, said target package is installed. Thus, the installation success rate increases. In addition, unnecessary installation operations are avoided and system resources saved.

BRIEF DESCRIPTION OF THE DRAWINGS

[010] To more clearly describe the embodiments of the present disclosure or the existing technical solutions, the following gives an overview of the drawings needed to describe the embodiments or the existing technology. Obviously, the following drawings show only some of the embodiments of the present disclosure, and those of ordinary skill in the art can obtain other drawings based on these drawings without creative work.

[011] Figure 1 shows the flowchart of a first data processing method provided by the embodiments of the present disclosure.

[012] Figure 2 shows the flowchart of a second data processing method provided by the embodiments of the present disclosure.

[013] Figure 3 shows the flowchart of a third data processing method provided by the embodiments of the present disclosure.

[014] Figure 4 shows the flowchart of a fourth data processing method provided by the embodiments of the present disclosure.

[015] Figure 5 shows the flowchart of a fifth data processing method provided by the embodiments of the present disclosure.

[016] Figure 6 shows the structural diagram of a data processing device provided by the embodiments of the present disclosure.

[017] Figure 7 shows the structural diagram of another data processing device provided by the embodiments of the present disclosure.

[018] Figure 8 shows the structural diagram of an example terminal device for embodiments of the disclosure.

DETAILED DESCRIPTION OF THE DRAWINGS

[019] Reference throughout this specification to "embodiments," "an embodiment," "example embodiment," or the like in the singular or plural means that one or more particular features, structures, or characteristics described in connection with an embodiment is included in at least embodiments of the present disclosure. Thus, the appearances of the phrases "in embodiments" or "in an embodiment," "in an example embodiment," or the like in the singular or plural in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more embodiments.

[020] The terminology used in the description of the disclosure herein is for the purpose of describing particular examples only and is not intended to be limiting of the disclosure. As used in the description of the disclosure 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. Also, as

used in the description herein and throughout the claims that follow, the meaning of "in" includes "in" and "on" unless the context clearly dictates 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 "may include," "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.

[021] As used herein, the term "module" or "unit" may refer to, be part of, or include an Application Specific Integrated Circuit (ASIC); an electronic circuit; a combinational logic circuit; a field programmable gate array (FPGA); a processor (shared, dedicated, or group) that executes code; other suitable hardware components that provide the described functionality; or a combination of some or all of the above, such as in a system-on-chip. The term module or unit may include memory (shared, dedicated, or group) that stores code executed by the processor.

[022] The exemplary environment may include a server, a client, and a communication network. The server and the client may be coupled through the communication network for information exchange, such as sending/receiving identification information, sending/receiving data files such as splash screen images, etc. Although only one client and one server are shown in the environment, any number of terminals or servers may be included, and other devices may also be included.

[023] The communication network may include any appropriate type of communication network for providing network connections to the server and client or among multiple servers or clients. For example, communication network may include the Internet or other types of computer networks or telecommunication networks, either wired or wireless. In a certain embodiment, the disclosed methods and apparatus may be implemented, for example, in a wireless network that includes at least one client.

[024] In some cases, the client may refer to any appropriate user terminal with certain computing capabilities, such as a personal computer (PC), a work station computer, a server computer, a hand-held computing device (tablet), a smart phone or mobile phone, or any other user-side computing device. In various embodiments, the client may include a network access device. The client may be stationary or mobile.

[025] A server, as used herein, may refer to one or more server computers configured to provide certain server functionalities, such as database management and search engines. A server may also include one or more processors to execute computer programs in parallel.

[026] The solutions in the embodiments of the present disclosure are clearly and completely described in combination with the attached drawings in the embodiments of the present disclosure. Obviously, the described embodiments are only a part, but not all, of the embodiments of the present

disclosure. On the basis of the embodiments of the present disclosure, all other embodiments acquired by those of ordinary skill in the art under the precondition that no creative efforts have been made shall be covered by the protective scope of the present disclosure.

[027] In order to make the objectives, technical solutions, and advantages of the present disclosure more comprehensible, the present disclosure is further described in detail below with reference to embodiments and the accompanying drawings.

[028] Obviously, embodiments are only described partly below, rather than all of them. Any other embodiment made by person of skill in the art without creative labor is in protection of the disclosure.

[029] In conjunction with the drawings of the embodiments of the present disclosure, the following clearly and completely describes the technical solutions provided by the embodiments of the present disclosure. Obviously, the described embodiments are only some, but not all, of the embodiments of the present disclosure. All the other embodiments which are obtained by those of ordinary skill in the art on the basis of the embodiments of the present disclosure without creative work shall fall within the protection scope of the present disclosure.

[030] The embodiments of the present disclosure provide a data processing method, and said method is applicable to terminals such as smartphones and tablet PCs. As shown in Figure 1, said method comprises:

[031] Step 101: Verify a stored target package based on a preset encrypted hash function, the target package being a package sent by a network-side server according to a user request.

[032] Verification of the target package can determine whether the received target package is the package requested by the user. If the target package passes the verification, the verification is successful and the received target package is the package requested by the user. Otherwise, the verification fails and the received target package is not the package requested by the user.

[033] During the verification, the target package is encoded on the basis of the hash function to obtain a string. The network-side server encodes the package requested by the user based on the same hash function to obtain another string. The data encoded using the hash function is unique. Therefore, if the string obtained by means of encoding on the terminal is the same as the string obtained by means of encoding on the network-side server, the target package received by the terminal is the package requested by the user.

[034] The string obtained by means of encoding is a hash, which is a message digest. Generally, a hash has a fixed length, which is much smaller than that of the encoded package. A vigorously-encrypted hash must be irreversible. None of the original information about the encoded package can be deduced by using a hash result. Optionally, one-way hash functions include the MD5 and Secure Hash Algorithm (SHA).

[035] Step 102: If the verification is successful, perform error detection on the target package according to a preset error detection standard.

[036] The preset error detection standard is the same as the compression mode adopted to generate the target package. Preferably, error detection is performed on the target package based on the CRC. When error detection is performed on the basis of the CRC, a CRC algorithm is selected according to the number of bits of the system running on the terminal. For example, in the case of a 32-bit system, the CRC32 algorithm is selected, in the case of a 64-bit system, the CRC64 algorithm is selected.

[037] Optionally, error detection is performed on the target package based on parity check.

[038] Step 103: If the error detection is successful, check the validity of the target package by invoking a verification function, the validity check being configured to check whether the target package can be parsed.

[039] If an Android system runs on the terminal, a preset function in the Package Manager class is invoked. Based on a parameter, the function checks whether the target package can be parsed by the system. The preset function is the information acquisition function getPackageInfo in the Package Manager class.

[040] Step 104: If the validity check is successful, install the target package.

[041] When the target package is an APK, if the target package passes the checks performed in steps 101 to 103, the target package is installed.

[042] The data processing method provided by the present disclosure can be configured to verify a stored target package based on a preset encrypted hash function, said target package being a package sent by a network-side server according to a user request; if said verification is successful, perform error detection on said target package according to a preset error detection standard; if said error detection is successful, perform validity check on said target package by invoking a verification function, said validity check being configured to check whether said target package can be parsed; if said validity check is successful, install said target package. Verification of a stored target package based on a preset encrypted hash function can ensure that the downloaded target package is the requested package, namely, ensuring that the target package is unique. Error detection on said target package according to a preset error detection standard can ensure that the target package is integral. Validity check on said target package by invoking a verification function can ensure that the target package is valid. The existing art only checks either the integrity or the uniqueness of the target package. By performing uniqueness check, integrity check, and validity check on target packages, the present disclosure can improve the check efficiency, capable of eliminating, by a larger proportion compared with the existing art, the target packages that cannot be installed. If the target package passes the above-mentioned three checks, said target package is installed. Thus, the

installation success rate increases. In addition, unnecessary installation operations are avoided and system resources saved.

[043] The embodiments of the present disclosure provide another data processing method to further describe the method as shown in Figure 1. Said method, before step 101 "verifying a stored target package based on a preset encrypted hash function, said target package being a package sent by a network-side server according to a user request", further comprises:

[044] Step 202: Receive a user-trigged selection instruction, which is configured to select the target package to be downloaded.

[045] The user clicks the download link of the target package on the download page displayed on the terminal, triggering a selection instruction.

[046] Step 202: Send to the network-side server an acquisition request corresponding to the selection instruction, the acquisition request being configured to obtain the target package.

[047] When the user-triggered selection instruction is received, an acquisition request is sent to the network-side server to obtain the target data specified by the selection instruction. For example, when a user clicks a software download link, triggering a selection instruction, an acquisition request is sent to the network-side server to request the server for download of the package corresponding to the link.

[048] Step 203: Receive the target package and verification string sent by the network-side server, the verification string being a string generated by encoding the target package based on the preset encrypted hash function.

[049] Based on the preset encrypted hash function, the network-side server encodes the target package requested by the acquisition request to obtain a verification string, and sends the verification string along with the target package to the terminal.

[050] Step 204: Save the target package and verification string.

[051] On receiving the target package and verification string, the terminal saves the target package and verification string.

[052] The data processing method provided by the embodiments of the present disclosure can be configured to send an acquisition request to the network-side server according to the user request, receive and save the target package and verification string sent by the network-side server, providing an operation object for subsequently checking whether the target package is complete and valid.

[053] The embodiments of the present disclosure provide another data processing method to further describe the method as shown in Figure 1. As shown in Figure 3, step 101 of verifying a stored target package based on a preset encrypted hash function can be implemented as follows:

[054] Step 301: Encode a stored target package based on a preset encrypted hash function to obtain the target string.

[055] The preset encrypted hash functions may include MD5, MD4, MD3, and SHA-1.

[056] For example, a typical application of MD5 is to generate a message digest of a message, thus preventing message falsification. In the embodiments of the present disclosure, the message is the target package and the generated message digest is the target string. Treating the entire target package as a text message, MD5 uses an irreversible string conversion algorithm to generate a unique MD5 message digest, namely, the target string.

[057] Step 302: Check whether the target string matches the verification string.

[058] The network-side server uses the same MD5 algorithm to encode the requested package and obtain the verification string. Therefore, if the target string matches the verification string, the downloaded target package is consistent with the requested package.

[059] The data processing method provided by the embodiments of the present disclosure can be configured to encode the target package and obtain the target string. If the target string matches the verification string, the target package is consistent with the requested package.

[060] The embodiments of the present disclosure provide another data processing method to further describe the method as shown in Figure 1. As shown in Figure 4, step 102 of performing error detection on the target package according to a preset error detection standard can be implemented as follows:

[061] Step 401: Partition the target package to generate at least two target sub-packages.

[062] The target package is partitioned according to the specified data size. The format of each target sub-package obtained through partitioning is the same as the format of the target package. For example, after the target package, which is an APK, is partitioned, the format of each target sub-package is the same as that of the APK, namely, the *.zip format. The size of a target sub-package is decided by the memory capacity and the running capability of the terminal. For example, a 1 MB APK is partitioned into ten target sub-packages, each of which is 100 KB in size. In this case, the memory performs error detection on these ten target sub-packages respectively, shortening the time required for error detection compared with the error detection directly performed on the APK.

[063] Step 402: Perform error detection on each target sub-package based on a preset error detection standard.

[064] Parallel error detection or serial error detection is performed on each target sub-package based on a preset error detection standard.

[065] The format of each target sub-package is the same as the format of the target package. Therefore, a preset error detection standard is configured to perform error detection on both the target package and target sub-packages.

[066] In this case, step 103, namely, checking the validity of the target package by invoking a verification function if the error detection is successful, can be implemented as follows:

[067] Step 403: If the error detection on each target sub-package is successful, invoke a verification function to perform validity check on the target package.

[068] If the error detection on all the target sub-packages is successful, it is determined that the error detection on the target package is successful. In this case, a verification function is invoked to perform validity check on said target package.

[069] With the data processing method provided by the embodiments of the present disclosure, the target package can be partitioned into multiple target sub-packages so that each target sub-package is much smaller than the target package. Thus, the complexity of and system resource consumption in error detection are reduced to improve the efficiency of error detection.

[070] The embodiments of the present embodiment provide another data processing method to further describe the method as shown in Figure 1. As shown in Figure 5, said method further comprises:

[071] Step 151: Display an error report if the check fails.

[072] If the check is successful, step 102 is performed; if the check fails, step 151 is performed.

[073] Step 152: Display an error report if the error detection fails.

[074] If the error detection is successful, step 103 is performed; if the error detection fails, step 152 is performed.

[075] Step 153: Display an error report if the validity check fails, the error report being configured to inform the user that the package cannot be run.

[076] If the error detection is successful, step 104 is performed; if the error detection fails, step 153 is performed.

[077] An error report can contain audios, images, or text. For example, an error report is displayed in a pop-up window, showing the text "APK installation failed. Please download again."

[078] With the data processing method provided by the embodiments of the present disclosure, when verification, error detection, or validity check fails, an error report is displayed, informing the user about the installation of the target package; meanwhile, the installation of the original package is canceled to save system resources.

[079] Further, said step of verifying a stored target package based on a preset encrypted hash function comprises verifying the stored target package based on the MD5.

[080] Said step of performing error detection on said target package according to a preset error detection standard comprises performing error detection on said target package according to the CRC.

[081] Said step of invoking a verification function to perform validity check on said target package comprises performing validity check on said target APK by invoking a preset function in the Android Package Manager class.

[082] Said target package is an Android package.

[083] In a preferred embodiment of the present disclosure, if the target package is an APK, MD5 is used as the preset encrypted hash function; CRC is used as the preset error detection standard; the invoked verification function is a preset function in the Android Package Manager class.

[084] The embodiments of the present disclosure further provide a data processing device as shown in Figure 6. The device 600 includes a non-transitory storage medium 610 and a hardware processor 620. The non-transitory storage medium 610 is accessible to the hardware processor 620 and is configured to store units including:

[085] a verification unit 611, configured to verify a target package stored in the storage unit 6110 based on a preset encrypted hash function, said target package being a package sent by a network-side server according to a user request.

[086] an error detection unit 612, configured to, if the verification performed by said verification unit 611 is successful, perform error detection on said target package based on a preset error detection standard.

[087] a validity check unit 613, configured to, if the detection performed by said error detection unit 612 is successful, perform validity check on said target package by invoking a verification function, said validity check being configured to check whether said target package can be parsed.

[088] an installation unit 614, configured to, if the check performed by said validity check unit 613 is successful, install said target package.

[089] The data processing device 600 provided by the present disclosure can be configured to verify a stored target package based on a preset encrypted hash function, said target package being a package sent by a network-side server according to a user request; if said verification is successful, perform error detection on said target package according to a preset error detection standard; if said error detection is successful, perform validity check on said target package by invoking a verification function, said validity check being configured to check whether said target package can be parsed; if said validity check is successful, install said target package. Verification of a stored target package based on a preset encrypted hash function can ensure that the downloaded target package is the requested package, namely, ensuring that the target package is unique. Error detection on said target package according to a preset error detection standard can ensure that the target package is integral. Validity check on said target package by invoking a verification function can ensure that the target package is valid. The existing art only checks either the integrity or the uniqueness of the target package. By performing uniqueness check, integrity check, and validity check on target packages, the present disclosure can improve the check efficiency, capable of eliminating, by a larger proportion compared with the existing art, the target packages that cannot be installed. If the target package passes the above-mentioned three checks, said target package is installed. Thus, the

installation success rate increases. In addition, unnecessary installation operations are avoided and system resources saved.

[090] Further, as shown in Figure 7, the example device 600 may further include the receiving unit 615, the sending unit 616, the first report unit 617, the second report unit 618, and the third report unit 619.

[091] Said receiving unit 615 is configured to receive a user-trigged selection instruction, which is configured to select the target package to be downloaded.

[092] The sending unit 616 is configured to send to the network-side server an acquisition request corresponding to said selection instruction received by said receiving unit 615, said acquisition request being configured to obtain said target package.

[093] Said receiving unit 615 is further configured to receive the target package and verification string sent by the network-side server, said verification string being a string generated by encoding the target package based on the preset encrypted hash function.

[094] Said storage unit 6110 is further configured to store said target package and verification string received by said receiving unit 615.

[095] The data processing device 600 provided by the embodiments of the present disclosure can be configured to send an acquisition request to the network-side server according to the user request, receive and save the target package and verification string sent by the network-side server, providing an operation object for subsequently checking whether the target package is complete and valid.

[096] Further, said verification unit 611 comprises:

[097] an encoding sub-unit 6111, configured to encode a target package stored in the storage unit 6110 based on a preset encrypted hash function to obtain the target string;

[098] a verification sub-unit 6112, configured to check whether said target string obtained by said encoding sub-unit 6111 matches said verification string received by the receiving unit 615.

[099] The data processing device 600 provided by the embodiments of the present disclosure can be configured to encode the target package and obtain the target string. If the target string matches the verification string, the target package is consistent with the requested package.

[0100] Further, said error detection unit 612 comprises:

[0101] a partition sub-unit 6121, configured to partition said target package to generate at least two target sub-packages;

[0102] a detection sub-unit 6122, configured to perform error detection on each of the target sub-packages obtained by partitioning each of said sub-units based on a preset error detection standard.

[0103] Said validity check unit 613 is further configured to, if the detection sub-unit detects that the error detection on each target sub-package is successful, perform validity check on said target package by invoking a verification function.

[0104] With the data processing device 600 provided by the embodiments of the present disclosure, the target package can be partitioned into multiple target sub-packages so that each target sub-package is much smaller than the target package. Thus, the complexity of and system resource consumption in error detection are reduced to improve the efficiency of error detection.

[0105] Said device 600 further comprises:

[0106] a first report unit 617, configured to display an error report if the verification performed by said verification unit 611 fails;

[0107] a second report unit 618, configured to display an error report if the error detection performed by said error detection unit 612 fails;

[0108] a third report unit 619, configured to display an error report if the check performed by said validity check unit 613 fails, said error report being configured to inform the user that the package cannot be run.

[0109] With the data processing device 600 provided by the embodiments of the present disclosure, when verification, error detection, or validity check fails, an error report is displayed, informing the user about the installation of the target package; meanwhile, the installation of the original package is canceled to save system resources.

[0110] Further, said verification unit 611 is configured to verify the stored target package based on MD5.

[0111] Said error detection unit 612 is further configured to perform error detection on said target package based on the CRC.

[0112] Said validity check unit 613 is further configured to perform validity check on said target APK by invoking a preset function in the Android Package Manager class.

[0113] Those of ordinary skill in the existing art can clearly understand that, for convenience and brevity of description, examples are given only based on the division of the function modules. In actual application, the above-mentioned functions can be allocated as needed to different function modules for completion. That is, the internal structure of the device can be divided into different function modules to complete all or some of the above-mentioned functions. For details about the working processes of the above-mentioned systems, devices, and units, see the description of the corresponding processes in the above-mentioned method embodiments.

[0114] While the present disclosure has been particularly disclosed and described above with reference to embodiments, it should be understood that the description is not intended to limit the

present disclosure. Various modifications and alterations may be made by those skilled in the present art without departing from the spirit and scope of the present disclosure as defined by the Claims.

[0115] With further reference to Figure 8, which shows the structural diagram of an example terminal device for embodiments of the disclosure,

[0116] Figure 8 is a block diagram of a partial device related to a terminal device such as a mobile phone. For example, the terminal device includes a radio frequency (RF) circuit 510, a memory 520, an input unit 530, a display unit 540, a sensor 550, an audio circuit 560, a wireless fidelity (WiFi) module 570, a processor 580, and a power 590, etc.. It's understood for persons skilled in the art that, the structure of a terminal device illustrated in Figure 8 is not limited, some components can be added or omitted, or some combinations or arrangement can be included.

[0117] Following is a detailed description of the structure of the terminal device by combining with Figure 8.

[0118] The RF circuit 510 is configured to receive and sending signals during calling or process of receiving and sending message. Specially, the RF circuit 510 will receive downlink information from the base station and send it to the processor 580; or send uplink data to the base station. Generally, the RF circuit 510 includes, but is not limited to, an antenna, at least one amplifier, a transceiver, a coupler, a low noise amplifier (LNA), a diplexer, and the like. In addition, the RF circuit 40 can communicate with network or other devices by wireless communication. Such wireless communication can use any one communication standard or protocol, which includes, but is not limited to, Global System of Mobile communication (GSM), (General Packet Radio Service, GPRS), (Code Division Multiple Access, CDMA), (Wideband Code Division Multiple Access, WCDMA), (Long Term Evolution, LTE), email, or (Short Messaging Service, SMS).

[0119] The memory 520 is configured to store software program and module which will be run by the processor 580, so as to perform multiple functional applications of the terminal device and data processing. The memory 530 mainly includes storing program area and storing data area. For example, the storing program area can store the operating system, at least one application program with required function (such as sound playing function, image playing function, etc.). The storing data area can store data established by terminal device according to actual using demand (such as audio data, phonebook, etc.) Furthermore, the memory 520 can be high-speed random access memory, or nonvolatile memory, such as disk storage, flash memory device, or other volatile solid-state memory devices.

[0120] The input unit 530 is configured to receive the entered number or character information, and the entered key signal related to user setting and function control of the terminal device 500. For example, the input unit 530 includes at least one of: a touch panel 531, other input devices 532, and a camera 533.

[0121] The touch panel 531 may include a touch screen, which can collect user's touch operations thereon or nearby (for example the operations generated by fingers of user or stylus pen, and the like, touching on the touch panel 531 or touching near the touch panel 531), and drive the corresponding connection device according to the preset program. Optionally, the touch panel 531 includes two portions including a touch detection device and a touch controller. Specifically, the touch detection device is configured to detect touch position of the user and detecting signals accordingly, and then sending the signals to the touch controller. Subsequently, the touch controller receives touch information from the touch detection device, and converts it to contact coordinates which are to be sent to the processor 580, and then receives command sent by the processor 580 to perform. In addition, the touch panel 531 can be implemented is forms of resistive type, capacitive type, infrared type and surface acoustic wave type. Besides the touch panel 531, the input unit 530 can include, but is not limited to other input devices 532, such as one or more selected from physical keyboard, function keys (such as volume control keys, switch key-press, etc.), a trackball, a mouse, and an operating lever, etc.. The camera 533 may be an optical device configured to record images in a digital format.

[0122] The display unit 540 is configured to display information entered by the user or information supplied to the user, and menus of the terminal device. For example, the display unit 540 includes a display panel 541, such as a Liquid Crystal Display (LCD), or an Organic Light-Emitting Diode (OLED). Furthermore, the display panel 541 can be covered by the touch panel 531, after touch operations are detected on or near the touch panel 531, they will be sent to the processor 580 to determine the type of the touching event. Subsequently, the processor 580 supplies the corresponding visual output to the display panel 541 according to the type of the touching event. As shown in Figure 8, the touch panel 531 and the display panel 541 are two individual components to implement input and output of the terminal device, but they can be integrated together to implement the input and output in some embodiments.

[0123] Furthermore, the terminal device 500 includes at least one sensor 550, such as light sensors, motion sensors, or other sensors. Specifically, the light sensors includes ambient light sensors for adjusting brightness of the display panel 541 according to the ambient light, and proximity sensors for turning off the display panel 541 and/or maintaining backlight when the terminal device is moved to the ear side. Accelerometer sensor as one of the motion sensors can detect the magnitude of accelerations in every direction (Triaxial, generally), and detect the magnitude and direction of gravity in an immobile status, which is applicable to applications of identifying attitudes of the mobile (such as switching between horizontal and vertical screens, related games, magnetometer attitude calibration, etc.), vibration recognition related functions (such as pedometer, percussion, etc.). And the terminal device 500 also can configure other sensors (such as

gyroscopes, barometers, hygrometers, thermometers, infrared sensors, etc.) whose detailed descriptions are omitted here.

[0124] The audio circuit 560, the speaker 561 and the microphone 562 supply an audio interface between the user and the terminal device. Specifically, the audio data is received and converted to electrical signals by audio circuit 560, and then transmitted to the speaker 561, which are converted to sound signal to output. On the other hand, the sound signal collected by the speaker is then converted to electrical signals which will be received and converted to audio data. Subsequently, the audio data are output to the processor 580 to process, and then sent to another terminal device via the RF circuit 510, or sent to the memory 520 to process further.

[0125] WiFi pertains to short-range wireless transmission technology providing a wireless broadband Internet, by which the terminal device can help the user to receive and send email, browse web, and access streaming media, etc.. Although the WiFi module 570 is illustrated in Figure 8, it should be understood that, WiFi module 570 is not a necessary for the terminal device, which can be omitted according the actual demand without changing the essence of the present disclosure.

[0126] The processor 580 is a control center of the terminal device, which connects with every part of the terminal device by various interfaces or circuits, and performs various functions and processes data by running or performing software program/module stored in the memory 520 or calling data stored in the memory 520, so as to monitor the terminal device. Optionally, the processor 580 may include one or more processing units. Preferably, the processor 580 can integrate with application processors and modem processors, for example, the application processors include processing operating system, user interface and applications, etc.; the modern processors are used for performing wireless communication. It can be understood that, it's an option to integrate the modern processors to the processor 580.

[0127] The processor 580 is configured to control a photographic equipment such as the camera 533 to scan target picture and analyze the target picture on basis of preset graphic code processing library; on condition that matched graphic code information is obtained in the analysis, determine the target picture as graphic code and transmit the matched graphic code information obtained in the analysis; on condition that the analysis fails, photograph the target picture to obtain a photo under identification comprising the target picture, transmit the photo under identification to server and receive the information of content matched with features of the identified picture and returned by the server after identification of picture features of the target picture.

[0128] The processor 580 is configured to control the display unit 540. The display 540 is configured to display the output of the matched graphic code information obtained in the analysis or display the content information returned by the server and matched with picture features of identified picture.

[0129] Furthermore, the terminal device 500 may include a power supply (such as battery) supplying power for each component, preferably, the power supply can connect with the processor 580 by power management system, so as to manage charging, discharging and power consuming.

[0130] In addition, the terminal device 500 may include a Bluetooth module and other hardware circuits, etc., which are not illustrated.

[0131] Person of skill in the art can get aware that the whole or part of method in embodiments above may be realized through relevant hardware under instruction of computer program, in which the program may be stored in a computer-readable memory medium. When the program is executed, flow processes in embodiments of method above may be contained. Therein, the memory medium above may be diskette, optical disk, Read-Only Memory (ROM) or Random Access Memory (RAM), or the like.

[0132] All disclosures above are just some of the preferred embodiments of the disclosure, which are descried specifically and particularly but not intending to limit the range of the disclosure. It should be noticed that person of skill in the art can make various changes and modifications within the scope of the disclosure, therefore, the protection scope of the present disclosure is defined by the claims.

Claims

1. A method for data processing, comprising:

verifying, by a device comprising a processor, a target package based on a preset encrypted hash function;

if said verification is successful, performing error detection on said target package according to a preset error detection standard;

if said error detection is successful, checking the validity of said target package by invoking a verification function configured to check whether said target package can be parsed; and

if said validity check is successful, installing said target package to the device.

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

receiving a user-trigged selection instruction configured to select the target package to be downloaded;

sending to a network-side server an acquisition request corresponding to said selection instruction, said acquisition request being configured to obtain said target package;

receiving the target package and a verification string sent by the network-side server, said verification string being a string generated by encoding the target package based on the preset encrypted hash function; and

saving said target package and verification string.

3. The method according to claim 2, wherein said step of verifying a stored target package based on the preset encrypted hash function comprises:

encoding a stored target package based on a preset encrypted hash function to obtain the target string; and

checking whether said target string matches said verification string.

4. The method according to claim 3, wherein said step of performing error detection on said target package according to a preset error detection standard comprises:

partitioning said target package to generate at least two target sub-packages; and

performing error detection on each target sub-package based on a preset error detection standard, and

wherein said step of, if said error detection is successful, checking the validity of said target package by invoking a verification function comprises:

if the error detection on each target sub-package is successful, invoking a verification function to perform validity check on said target package.

5. The method according to claim 4, further comprising:

displaying an error report if said check fails;

displaying an error report if said error detection fails; and

displaying an error report if said validity check fails, said error report being configured to inform the user that the package cannot be run.

6. The method according to any of claims 1 to 5, wherein:

said step of verifying a stored target package based on a preset encrypted hash function comprises:

verifying a stored target package based on the Message Digest Algorithm 5 (MD5);

said step of performing error detection on said target package according to a preset error detection standard comprises:

performing error detection on said target package based on a cyclic redundancy check (CRC);

said step of invoking a verification function to perform validity check on said target package comprises:

invoking a preset verification function to perform validity check on said target package.

7. A device for data processing, comprising a hardware processor and a non-transitory storage medium configured to store units comprising:

a verification unit, configured to verify a target package stored in the storage unit based on a preset encrypted hash function, said target package being a package sent by a network-side server according to a user request;

an error detection unit, configured to, if the verification performed by said verification unit is successful, perform error detection on said target package based on a preset error detection standard;

a validity check unit, configured to, if the detection performed by said error detection unit is successful, perform validity check on said target package by invoking a verification function, said validity check being configured to check whether said target package can be parsed; and

an installation unit, configured to, if the check performed by said validity check unit is successful, install said target package.

8. The device according to claim 7, wherein said non-transitory storage medium further configured to store:

a receiving unit, configured to receive a user-trigged selection instruction, which is configured to select the target package to be downloaded;

a sending unit, configured to send to the network-side server an acquisition request corresponding to said selection instruction received by said receiving unit, said acquisition request being configured to obtain said target package;

said receiving unit is further configured to receive the target package and verification string sent by the network-side server, said verification string being a string generated by encoding the target package based on the preset encrypted hash function; and

said storage unit is further configured to store said target package and verification string

received by said receiving unit.

9. The device according to claim 8, wherein said verification unit comprises:

an encoding sub-unit, configured to encode a target package stored in the storage unit based on a preset encrypted hash function to obtain the target string; and

a verification sub-unit, configured to check whether said target string obtained by said encoding sub-unit matches said verification string received by the receiving unit.

10. The device according to claim 9, wherein said error detection unit comprises:

a partition sub-unit, configured to partition said target package to generate at least two target sub-packages; and

a detection sub-unit, configured to perform error detection on each of the target sub-packages obtained by partitioning each of said sub-units based on a preset error detection standard;

wherein aid validity check unit is further configured to, if the detection sub-unit detects that the error detection on each target sub-package is successful, perform validity check on said target package by invoking a verification function.

11. The device according to claim 10, further comprising:

a first report unit, configured to display an error report if the verification performed by said verification unit fails;

a second report unit, configured to display an error report if the detection performed by said error detection unit fails;

a third report unit, configured to display an error report if the check performed by said validity check unit fails, said error report being configured to inform the user that the package cannot be run.

12. The device according to any of claims 7 to 11, wherein said verification unit is further configured to verify a stored target package based on Message Digest Algorithm 5 (MD5);

said error detection unit is further configured to perform error detection on said target package based on a cyclic redundancy check (CRC);

said validity check unit is further configured to perform validity check on said target package by invoking a preset function.

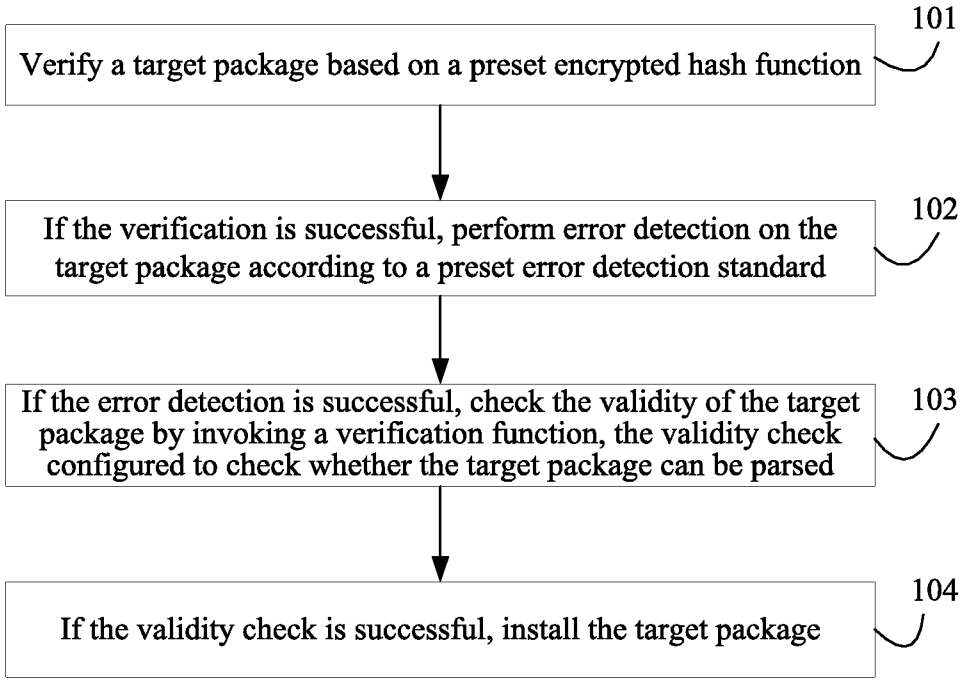

Figure 1

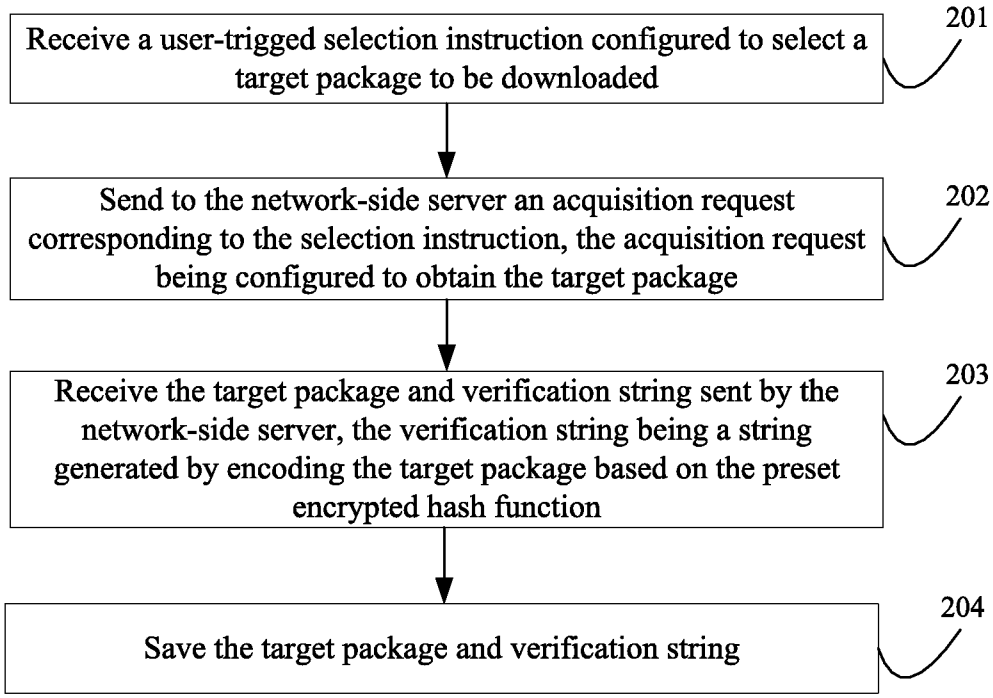

Figure 2

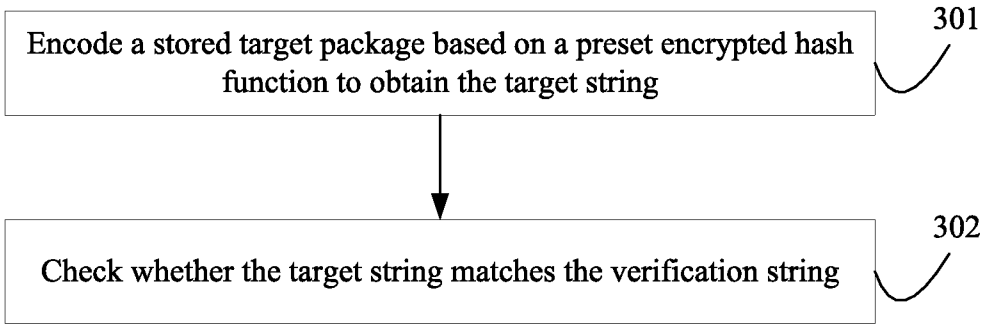

Figure 3

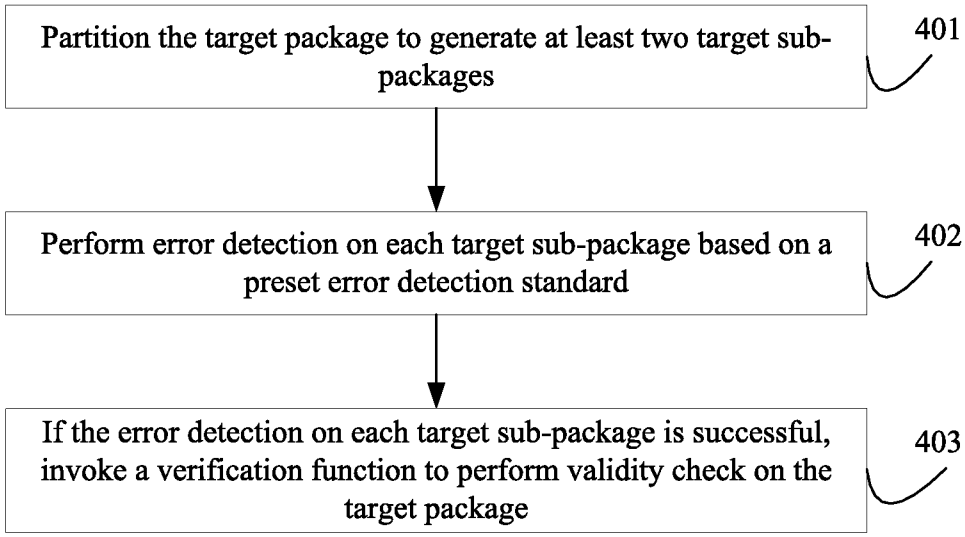

Figure 4

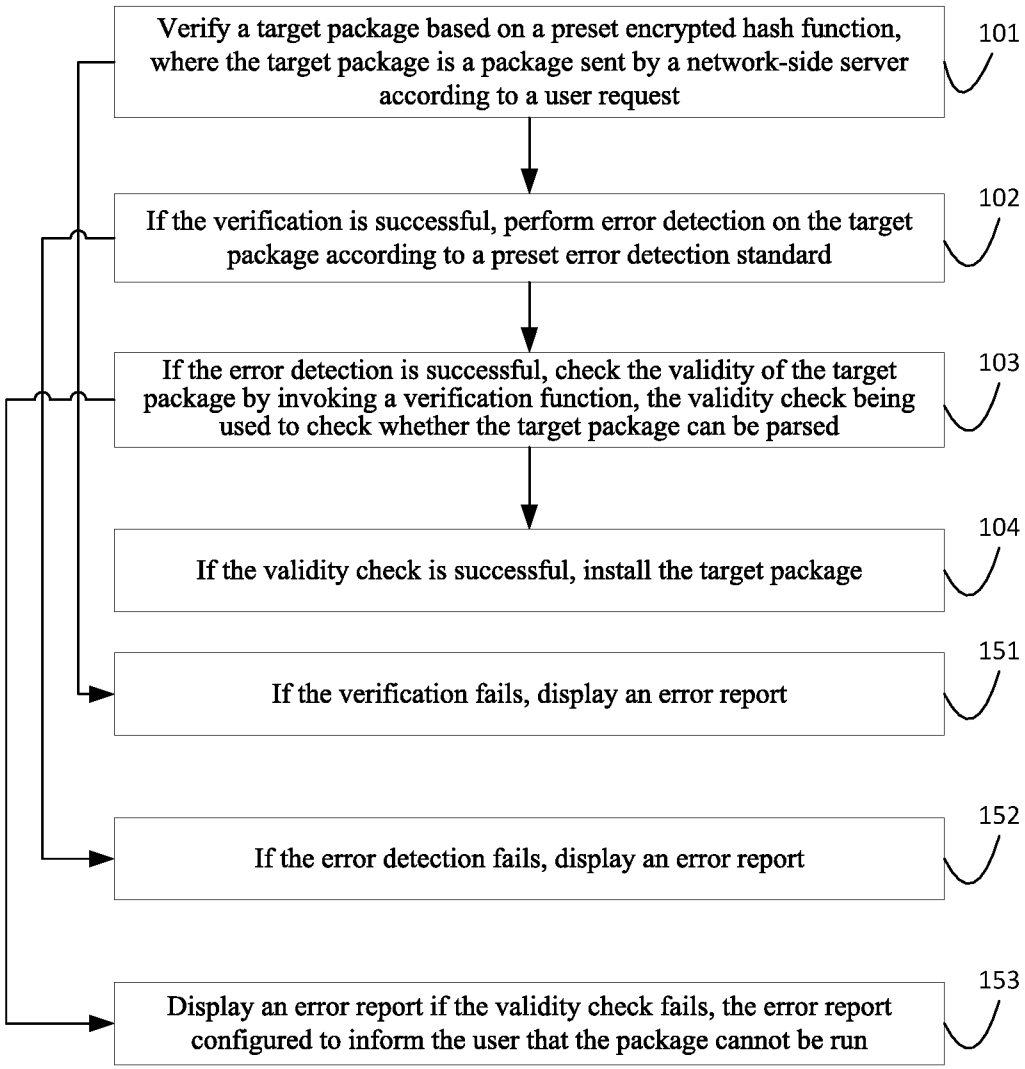
Verify a target package based on a preset encrypted hash function, where the target package is a package sent by a network-side server according to a user request
101
If the verification is successful, perform error detection on the target package according to a preset error detection standard
102
If the error detection is successful, check the validity of the target package by invoking a verification function, the validity check being used to check whether the target package can be parsed
103
If the validity check is successful, install the target package
104
If the verification fails, display an error report
151
If the error detection fails, display an error report
152
Display an error report if the validity check fails, the error report configured to inform the user that the package cannot be run
153

Figure 5

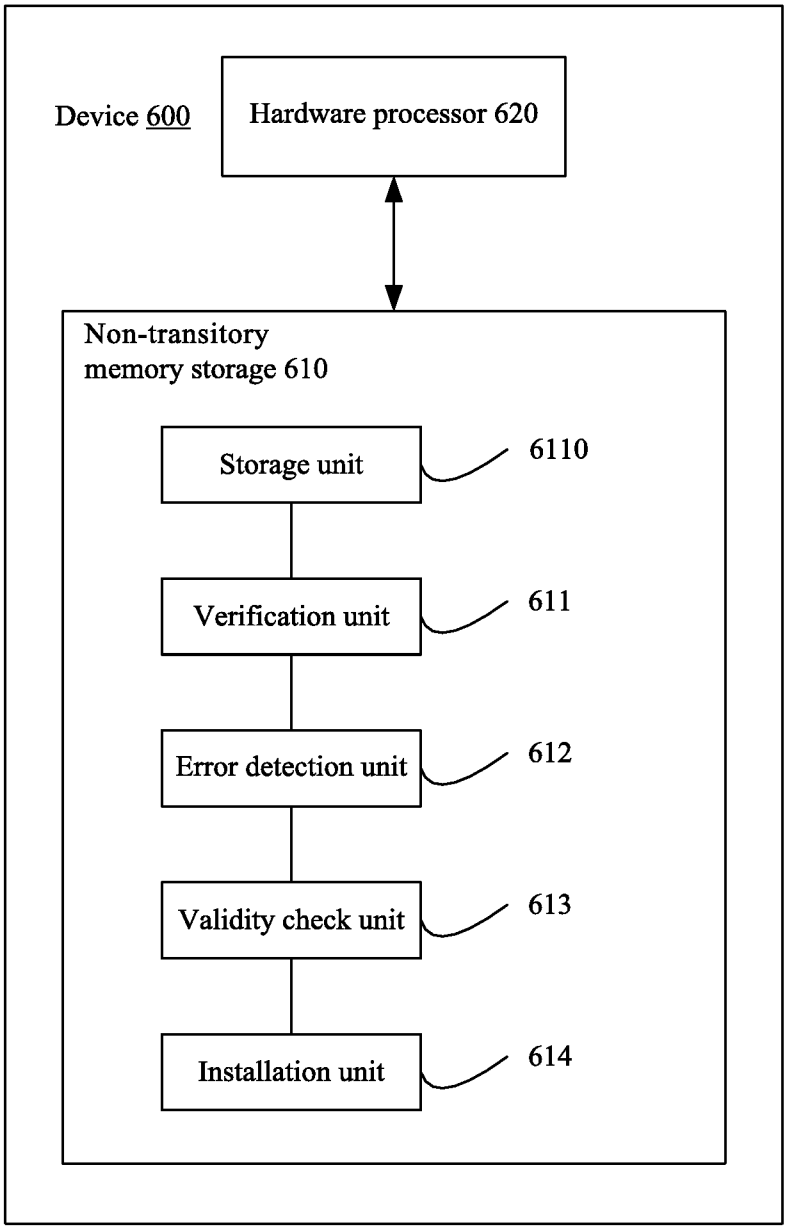
Device 600
Hardware processor 620
Non-transitory
memory storage 610
Storage unit
6110
Verification unit
611
Error detection unit
612
Validity check unit
613
Installation unit
614

Figure 6

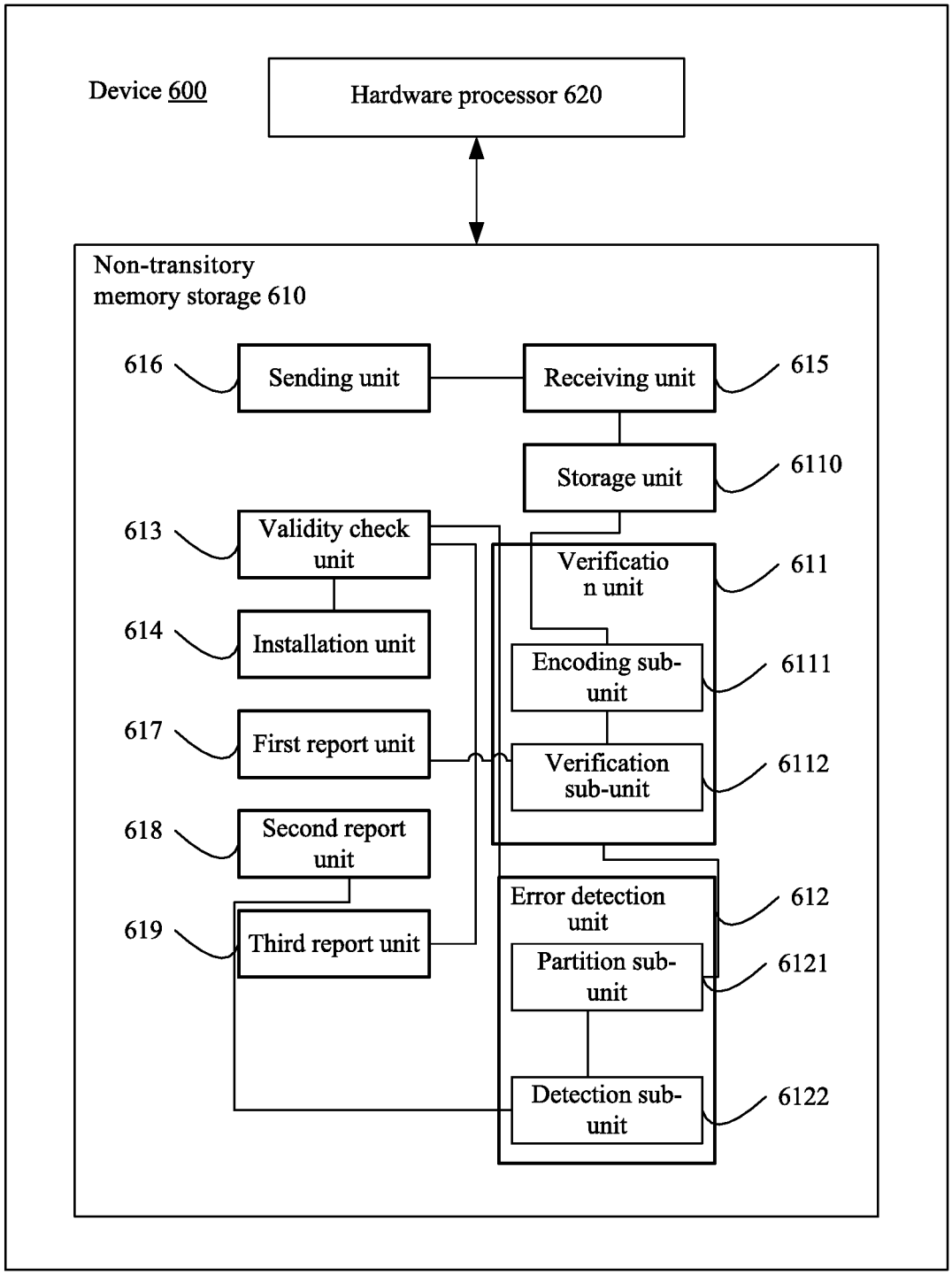
Device 600
Hardware processor 620
Non-transitory memory storage 610
616
Sending unit
Receiving unit
615
Storage unit
6110
613
Validity check unit
Verification unit
611
614
Installation unit
Encoding sub-unit
6111
617
First report unit
Verification sub-unit
6112
618
Second report unit
Error detection unit
612
619
Third report unit
Partition sub-unit
6121
Detection sub-unit
6122

Figure 7

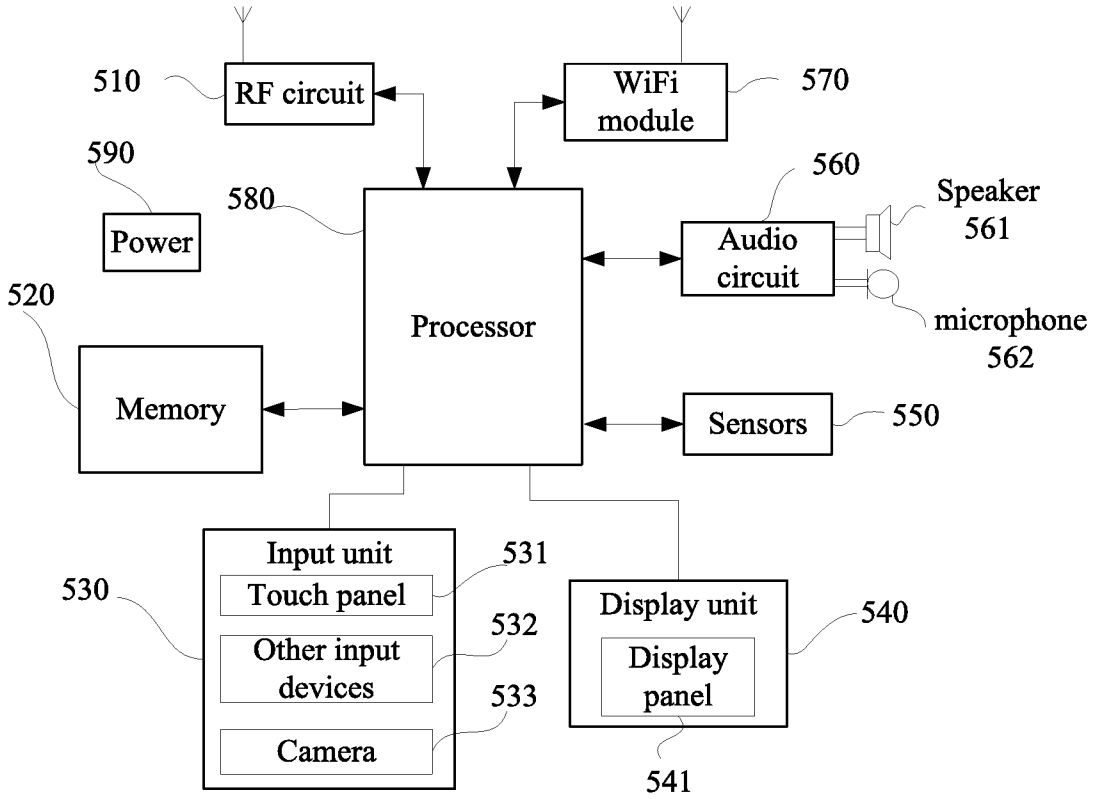
510
RF circuit
WiFi module
570
590
Power
580
560
Audio circuit
Speaker
561
microphone
562
520
Processor
Memory
Sensors
550
Input unit
531
530
Touch panel
532
Other input devices
533
Camera
Display unit
540
Display panel
541

Figure 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/083515

A. CLASSIFICATION OF SUBJECT MATTER

H04L 1/00(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)

H04L

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)

CPRSABS;CNTXT;CNKI;VEN: data, packet, package, integrity, validity, install, error, unique, CRC,detect+, APK, encrypt, hash, parse

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102087605 A (YULONG COMPUTER TELECOM TECHNOLOGY SHENZHEN CO., LTD.) 08 June 2011 (2011-06-08) the whole document	1-12
A	CN 101990239 A (ZTE CORP.) 23 March 2011 (2011-03-23) the whole document	1-12
A	CN 102034058 A (CHINA UNITED NETWORK COMMUNICATION GROUP CO., LTD.) 27 April 2011 (2011-04-27) the whole document	1-12
A	CN 101895457 A (HUIXIONG BEIJING SCI&TECHNOLOGY CO., LTD.) 24 November 2010 (2010-11-24) the whole document	1-12

☐ 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
22 October 2014	**26 November 2014**

Name and mailing address of the ISA/CN	Authorized officer
STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA(ISA/CN) **6,Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088 China**	**ZHOU,Dan**
Facsimile No. **(86-10)62019451**	Telephone No. **(86-10)62089390**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/083515

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 102087605 A	08 June 2011	CN 102087605 B	07 May 2014
CN 101990239 A	23 March 2011	Non e	
CN 102034058 A	27 April 2011	CN 102034058 B	21 August 2013
CN 101895457 A	24 November 2010	Non e	