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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 September 2016 (09.09.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/140947 A1

(51) International Patent Classification:
G06F 21/36 (2013.01) *H04L 9/32* (2006.01)
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/US2016/020214

(22) International Filing Date:
1 March 2016 (01.03.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201510094744.9 3 March 2015 (03.03.2015) CN

(71) Applicant: **ALIBABA GROUP HOLDING LIMITED** [—/US]; Fourth Floor, One Capital Place, P.O.Box 847, George Town, Grand Cayman (KY).

(72) Inventor: **ZHANG, Jie**; Alibaba Group Legal Department, 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou 311121 (CN).

(74) Agent: **CHEN, Weiguo**; Finnegan, Henderson, Farabow, Garrett &, Dunner LLP, 901 New York Avenue, NW, Washington, DC 20001-4413 (US).

(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, 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, ST, 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,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR USER IDENTITY AUTHENTICATION

(57) Abstract: A method for user identity authentication is provided. The method includes receiving an authentication image selected by a user, and acquiring, based on the authentication image, a password to be verified. The method may further include acquiring a preset verification password, and comparing the verification password with the password to be verified to obtain a user identity authentication result.

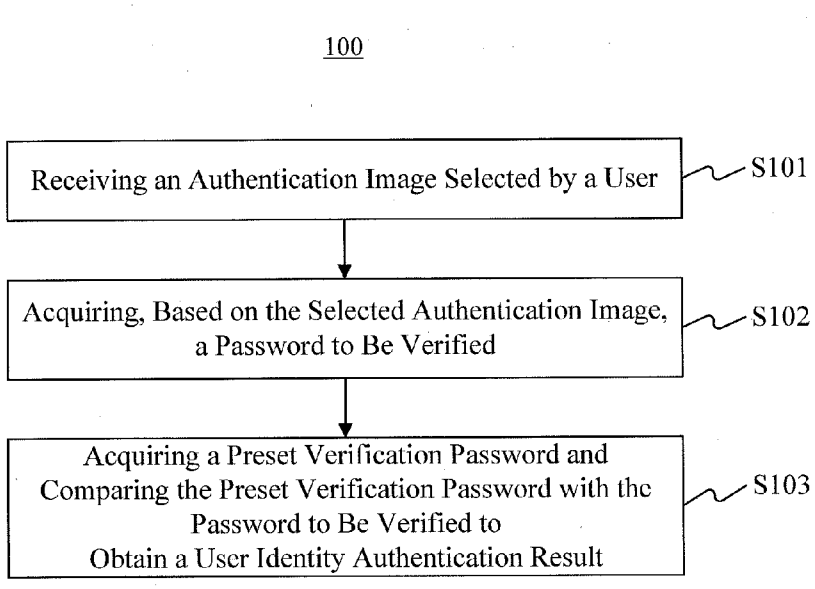

Fig. 1

WO 2016/140947 A1

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))*

METHOD AND APPARATUS FOR USER IDENTITY AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATION

[001] This application is based upon and claims priority to Chinese Patent Application No. 201510094744.9, filed March 3, 2015, the entire contents of which are incorporated herein by reference.

TECHNICAL FIELD

[002] The present application relates to the technical field of network security and, more particularly, to a method and an apparatus for user identity authentication.

BACKGROUND

[003] Conventionally, a terminal device performs user identity authentication by users manually inputting character strings, such as numbers and letters.

[004] However, authentication passwords in the form of numbers and letters may not be memorized conveniently and therefore are often be forgotten by users. Moreover, the operation of inputting these passwords is relatively cumbersome.

SUMMARY

[005] The present disclosure provides a method for user identity authentication. Consistent with some embodiments, the method includes receiving an authentication image selected by a user, and acquiring, based on the authentication image, a password to be verified. The method may further include acquiring a preset verification password, and comparing the verification password with the password to be verified to obtain a user identity authentication result.

[006] Consistent with some embodiments, this disclosure provides an apparatus for

user identity authentication. The apparatus includes a receiving module configured to receive an authentication image selected by a user and an acquiring module configured to acquire, based on the authentication image, a password to be verified. The apparatus may further include a verification module configured to acquire a preset verification password and compare the verification password with the password to be verified to obtain a user identity authentication result.

[007] Consistent with some embodiments, this disclosure provides a non-transitory computer-readable storage medium having stored therein instructions. When executed by a processor in a device, the instructions cause the device to perform operations including receiving an authentication image selected by a user, acquiring, based on the authentication image, a password to be verified, acquiring a preset verification password, and comparing the verification password with the password to be verified to obtain a user identity authentication result.

[008] Additional objects and advantages of the disclosed embodiments will be set forth in part in the following description, and in part will be apparent from the description, or may be learned by practice of the embodiments. The objects and advantages of the disclosed embodiments may be realized and attained by the elements and combinations set forth in the claims.

[009] It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the disclosed embodiments, as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[010] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate embodiments consistent with the invention and, together with the description, serve to explain the principles of the invention.

[011] Fig. 1 is a flowchart of an exemplary method for user identity authentication, consistent with some embodiments of this disclosure.

[012] Fig. 2 is a schematic diagram of authentication images displayed to a user, consistent with some embodiments of this disclosure.

[013] Fig. 3 is a flowchart of another exemplary method for user identity authentication, consistent with some embodiments of this disclosure.

[014] Fig. 4 is a block diagram of an exemplary apparatus for user identity authentication, consistent with some embodiments of this disclosure.

[015] Fig. 5 is a block diagram of another exemplary apparatus for user identity authentication, consistent with some embodiments of this disclosure.

DESCRIPTION OF THE EMBODIMENTS

[016] Reference will now be made in detail to exemplary embodiments, examples of which are illustrated in the accompanying drawings. The following description refers to the accompanying drawings in which the same numbers in different drawings represent the same or similar elements unless otherwise represented. The implementations set forth in the following description of exemplary embodiments do not represent all implementations consistent with the invention. Instead, they are merely examples of devices and methods consistent with aspects related to the invention as recited in the appended claims.

[017] Fig. 1 is a flowchart of an exemplary method 100 for user identity authentication, consistent with some embodiments of this disclosure. The exemplary method 100 may be performed by a terminal device. Referring to Fig. 1, the method 100 includes the following steps.

[018] In step S101, the terminal device receives an authentication image selected by a user. Fig. 2 is a schematic diagram 200 of authentication images displayed to a user, consistent with some embodiments of this disclosure. For example, an application program of

the terminal device may obtain a plurality of authentication images as selectable images and display them on a display of the terminal device. Subsequently, the user may select, from the displayed authentication images, the image preset as a password image so as to perform identity authentication.

[019] In some embodiments, the authentication images may be randomly selected from all of the images stored in the terminal device and may be randomly arranged.

[020] The image that is preset as a password image may be placed at a random position in authentication images. In some implementations, the password image may be placed at the first page or the first few pages of all authentication images so that a user may conveniently find the password image.

[021] In step S102, the terminal device acquires, based on the selected authentication image, a password that is to be verified. For example, a password may be acquired by a preset algorithm according to an image selected by a user.

[022] In some embodiments, the terminal device may acquire a pre-stored hash key and perform hash operation according to the hash key and the selected authentication image to obtain the password.

[023] In some embodiments, before selecting the authentication image, the user may preset a verification password in advance. For example, an application program of the terminal device may obtain a plurality of images from a terminal device and display the images to a user in a randomly arranged manner so as to allow the user to select an image as a password image. The terminal device may then generate a random number as a hash key according to the password image, and generate a verification password by the hash key and a preset hash algorithm (e.g., SHA-256 algorithm and the like). The terminal device may then securely store the random number and the verification password in a secure storage area of the terminal device so that comparative verification may be performed when identity

verification is required. For example, the operation of storing the random number and the verification password may be performed after detection by a preset secure detection program. A secure storage area, for example, may be a storage area where restriction or encryption of the access authority is implemented.

[024] During verification of user identity, the terminal device may acquire the pre-stored random number as a hash key, and perform the hash operation according to the hash key and the authentication image selected by a user, thereby obtaining a password to be verified. The hash operation herein may be the same as the hash algorithm used when a verification password is set. In doing so, the password obtained by the same hash key may be the same as the preset verification password when the image selected by a user is the same as the preset password image.

[025] In step S103, the terminal device acquires a preset verification password and compares the preset verification password with the password to be verified to obtain a user identity authentication result.

[026] For example, a preset verification password may be acquired and then compared with a password to be verified. If the password to be verified is consistent with the preset verification password, identity authentication may be determined to be successful. Otherwise, identity authentication may be determined to fail.

[027] In the method 100 described above, a password is generated according to an image selected by a user, and compared with a preset verification password to verify user identity. The user is required to select, from randomly arranged images, an image used when a verification password is set to complete identity authentication, thereby providing simple and convenient operation. Moreover, a password image may be memorized conveniently by the user.

[028] Fig. 3 is a flowchart of another exemplary method 300 for user identity

authentication, consistent with some embodiments of this disclosure. The exemplary method 300 may be performed by a terminal device. Referring to Fig. 3, the method 300 includes the following steps.

[029] In step S201, the terminal device generates a verification password, and stores the verification password and a hash key used for generating the verification password.

[030] For example, an application program may obtain a plurality of images from a terminal device and display the images to a user in a randomly arranged manner to allow the user to select one image as a password image. The application program may generate a random number according to the password image, use the random number as a hash key, and generate a verification password by the hash key and a preset hash algorithm (e.g., SHA-256 algorithm and the like). Subsequently, the application program may securely store the random number and the generated verification password in a secure storage area of the terminal device so that comparison may be performed when identity authentication is required.

[031] The operation of storing the random number and the verification password may be performed after detection by a preset secure detection program. A secure storage area, for example, may be a storage area where restriction or encryption of the access authority is implemented. In addition, the random number and verification password may also be stored by an existing or possible future security technique, which is not intended to be limited by the present disclosure.

[032] In step S202, when a user is required to input a password, the terminal device displays selectable authentication images to the user, so that the user may select an image from the displayed images. In some embodiments, the authentication images may be randomly selected from all images in the terminal device and may be randomly arranged on a display of the terminal device.

[033] As shown in Fig. 2, an application program may obtain all images from a

terminal device for random arrangement, or randomly select a subset of the images for arrangement as authentication images to a user, where the authentication images include a password image used for setting a verification password.

[034] In some embodiments, the image preset as a password image may be placed at a random position in the authentication images. In other embodiments, the image preset as a password image may be placed at the first page or the first few pages of the authentication images so that a user may conveniently find the image.

[035] In step S203, the terminal device receives an authentication image selected by the user. For example, a user may select the image preset as a password image from the authentication images to perform identity authentication.

[036] In step S204, the terminal device acquires a password to be verified based on the authentication image selected by a user and a pre-stored hash key.

[037] For example, a pre-stored random number may be acquired as a hash key, and a hash operation may be performed according to the hash key and the image, thereby obtaining the password to be verified. The hash operation herein may be the same as a hash algorithm used when a verification password is set, and thus a password to be verified may be the same as a preset verification password where an image selected by a user is the same as a password image used when a password is set.

[038] In step S205, the terminal device acquires a preset verification password and compares the preset verification password with the password to be verified to obtain a user identity authentication result. If the password to be verified is consistent with the preset verification password, identity authentication may be determined to be successful. Otherwise, identity authentication may be determined to fail.

[039] In some embodiments, a backup character string password may be preset. When a user forgets or deletes the image for verification, the user may be prompted to input a

character string for verifying identity. Identity authentication may be performed according to a preset character string password, and the password image and the verification password may be reset after authentication is passed. For example, a password image may be reselected according to step S201, and an updated verification password may be generated. Other types of identity authentication methods, such as performing verification by other pre-bound devices, may also be used when a user fails to input a correct password image. Other alternative identity authentication methods known to a person skilled in the art will not be described herein.

[040] In step S206, the terminal device resets the verification password if user identity authentication is passed.

[041] When a user desires to change a password image, the user may be first required to pass the above identity authentication. After the authentication is passed, the user may start a password modification process. For example, the user may reselect a password image according to step S201 to update a verification password.

[042] In the method 300 described above, a hash key and a verification password may be generated by a preset password image. In the course of verification, a password may be generated based on an authentication image selected by a user and a pre-stored hash key, and be compared with a preset verification password to verify user identity. The user is required to select, from randomly arranged authentication images, an authentication image used when a verification password is set to complete identity authentication, thereby providing simple and convenient operation. Moreover, a password image may be memorized conveniently by the user. Further, selectable authentication images may be randomly arranged in the course of verification, so as to prevent viruses such as Trojan horses from probing the user input, thereby improving the password security. In addition, when a user forgets a password image or the password image is deleted, identity authentication may also

be performed by other alternative methods so that a verification password may be reset, thereby improving the identity authentication efficiency.

[043] Fig. 4 is a block diagram of an exemplary apparatus 400 for user identity authentication, consistent with some embodiments of this disclosure. Referring to Fig. 4, the apparatus 400 includes a receiving module 410, an acquiring module 420, and a verification module 430.

[044] The receiving module 410 is configured to receive an authentication image selected by a user. For example, as shown in Fig. 2, authentication images may be obtained from a terminal device by an application program. The obtained images may be used as authentication images which are then displayed to a user (e.g., on a display of the terminal device), and the user may select the authentication image that is preset as a password image from the displayed images to perform identity authentication.

[045] In some embodiments, the authentication images may be randomly selected from all images stored in a terminal device and may be randomly arranged on a display of the terminal device.

[046] The authentication image preset as a password image may be placed at a random position in the displayed images. In some implementations, the password image may be placed at the first page or the first few pages of all displayed authentication images so that a user may conveniently find the image.

[047] The acquiring module 420 is configured to acquire a password to be verified based on the selected authentication image. In some embodiments, the acquiring module 420 may acquire a pre-stored random number as a hash key, and perform a hash operation based on the hash key and the image selected by a user, thereby obtaining a password to be verified.

[048] The verification module 430 is configured to acquire a preset verification password and compare the preset verification password with the password to be verified to

obtain a user identity authentication result. If the password to be verified is consistent with the preset verification password, the verification module 430 may determine the identity authentication to be successful. Otherwise, the verification module 430 may determine the identity authentication to fail.

[049] Fig. 5 is a block diagram of another exemplary apparatus 500 for user identity authentication, consistent with some embodiments of this disclosure. Referring to Fig. 5, the apparatus 500 includes a receiving module 410, an acquiring module 420, a verification module 430, an initializing module 540, a storing module 550, a display module 560, and a resetting module 570. The acquiring module 420 includes a first acquiring submodule 521 and a first processing submodule 522.

[050] The initializing module 540 is configured to set the verification password. As shown in Fig. 5, the initializing module 540 includes a second acquiring submodule 541, a generating submodule 542, and a second processing submodule 543. The second acquiring submodule 541 is configured to acquire an authentication image selected by a user for verification. The generating submodule 542 is configured to generate a random number. The second processing submodule 543 is configured to use the random number as a hash key, and perform a hash operation based on the hash key and the authentication image selected by the user to obtain a verification password.

[051] In some embodiments, an application program may obtain all images from a terminal device and display the images to a user in a randomly arranged manner to allow the user to select one image as a password image. The generating submodule 542 may be configured to generate a random number according to the password image. The second processing submodule 543 may be configured to use the random number as a hash key, and generate a verification password by the hash key and a preset hash algorithm (e.g., SHA-256 algorithm and the like).

[052] The storing module 550 is configured to store the random number and the verification password. The storing module 550 may be configured to securely store the random number and the generated verification password in a secure storage area of the terminal device, so that comparison may be performed for identity authentication.

[053] The operation of storing the random number and the verification password may be performed after detection by a preset secure detection program. A secure storage area, for example, may be a storage area where restriction or encryption of the access authority is implemented. In addition, the random number and verification password may also be stored by an existing or possible future security technique, which is not intended to be limited by the present disclosure.

[054] The display module 560 is configured to display selectable authentication images to a user when the user is required to input a password, so that the user may select an authentication image from the displayed images. The authentication images may be randomly selected from a subset of or all images in the terminal device and may be randomly arranged. As shown in Fig. 2, the display module 560 may obtain all images from a terminal device for random arrangement, or randomly select a subset of the images for arrangement as authentication images which are then displayed to a user, where the authentication images include a password image used for setting a verification password.

[055] In some embodiments, the display module 560 may be configured to place the image preset as a password image at a random position in the displayed images. In other embodiments, the image preset as a password image may be placed at the first page or the first few pages of the authentication images so that a user may conveniently find the image.

[056] In some embodiments, the authentication images may be transmitted in real time via networks, such as mobile data networks, WiFi, Bluetooth, infrared transmission, and so on. In some embodiments, when authentication images are transmitted in real time via

networks, the source of the authentication images may be designated by users. A terminal device may be configured to start a corresponding function for receiving the network images. For example, a user may enable an image receiving function of the terminal device, such that images may be transmitted in real time via the mobile data network.

[057] The first acquiring submodule 521 is configured to acquire a pre-stored hash key after receiving an authentication image selected by a user. The first processing submodule 522 is configured to perform a hash operation according to the hash key and the received image to obtain the password to be verified. The hash operation may be the same as a hash algorithm used for setting the verification password, such that a password to be verified may be the same as the preset verification password when the authentication image selected by a user is the same as the password image used to set the verification password.

[058] The resetting module 570 is configured to reset the verification password after user identity authentication is passed. When a user desires to replace a password image, the user may be first required to pass the above identity authentication. After the authentication is passed, the resetting module 570 may be configured to start a password modification process and prompt the user to reselect a password image so as to update a verification password.

[059] In some embodiments, a backup character string password may be preset. When a user forgets or deletes the password image, the verification module 430 may be configured to authenticate the user according to a preset character string, and reset the verification password after authentication is passed. Other types of identity authentication methods, such as performing verification by other pre-bound devices, may also be used when a user fails to input a correct password image. Other alternative identity authentication methods known to a person skilled in the art will not be described herein.

[060] In exemplary embodiments, a non-transitory computer-readable storage medium including instructions is also provided, and the instructions may be executed by a

device (such as a client terminal, a personal computer, or the like), for performing the above-described methods. The above-described methods may be implemented in a distributed computing environment, where one or more steps may be executed by a remote processing device connected through a network. The instructions executable by a device for performing the above-described methods may be stored in a local non-transitory computer-readable storage medium or in a computer-readable storage medium located in a remote device.

[061] It should be noted that, the relational terms herein such as "first" and "second" are used only to differentiate an entity or operation from another entity or operation, and do not require or imply any actual relationship or sequence between these entities or operations. Moreover, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items, or meant to be limited to only the listed item or items.

[062] The illustrated steps in the above-described figures are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. Thus, these examples are presented herein for purposes of illustration, and not limitation. For example, steps or processes disclosed herein are not limited to being performed in the order described, but may be performed in any order, and some steps may be omitted, consistent with disclosed embodiments.

[063] One of ordinary skill in the art will understand that the above described embodiments may be implemented by hardware, or software (program codes), or a combination of hardware and software. If implemented by software, it may be stored in the above-described computer-readable media. The software, when executed by the processor may perform the disclosed methods. If implemented by hardware, the above described

embodiments may be implemented by one of the following techniques known in the art or a combination thereof: a discrete logic circuit having a logic gate circuit for realizing a logic function of a data signal, an application specific integrated circuit having an appropriate combination logic gate circuit, a programmable gate array (PGA), a field programmable gate array (FPGA), etc. The computing units and the other functional units described in this disclosure may be implemented by hardware, or software, or a combination of hardware and software. One of ordinary skill in the art will also understand that multiple ones of the above described modules/units may be combined as one module/unit, and each of the above described modules/units may be further divided into a plurality of sub-modules/sub-units.

[064] Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed here. This application is intended to cover any variations, uses, or adaptations of the invention following the general principles thereof and including such departures from the present disclosure as come within known or customary practice in the art. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

[065] It will be appreciated that the present invention is not limited to the exact construction that has been described above and illustrated in the accompanying drawings, and that various modifications and changes may be made without departing from the scope thereof. It is intended that the scope of the invention should only be limited by the appended claims.

WHAT IS CLAIMED IS:

1. A method for user identity authentication, comprising:

receiving an authentication image selected by a user;

acquiring, based on the authentication image, a password to be verified;

acquiring a preset verification password; and

comparing the verification password with the password to be verified to obtain a user identity authentication result.

2. The method of claim 1, wherein acquiring the password to be verified comprises:

acquiring a pre-stored hash key; and

performing a hash operation based on the hash key and the authentication image to obtain the password to be verified.

3. The method of claim 1, further comprising setting the verification password before receiving the authentication image.

4. The method of claim 3, wherein setting the verification password comprises:

acquiring a password image selected by the user;

generating a random number as a hash key; and

performing a hash operation according to the hash key and the password image to

obtain the verification password.

5. The method of claim 1, further comprising:

displaying a plurality of selectable authentication images on a display of a terminal device before receiving the authentication image selected by the user.

6. The method of claim 1, further comprising:

after obtaining the user identity authentication result, resetting the verification password if user identity authentication is passed.

7. The method of claim 1, further comprising:

authenticating the user according to a preset character string; and

resetting the verification password after authentication is passed.

8. An apparatus for user identity authentication, comprising:

a receiving module configured to receive an authentication image selected by a user;

an acquiring module configured to acquire, based on the authentication image, a password to be verified; and

a verification module configured to:

acquire a preset verification password; and

compare the verification password with the password to be verified to obtain a user identity authentication result.

9. The apparatus of claim 8, wherein the acquiring module comprises:

a first acquiring submodule configured to acquiring a pre-stored hash key; and

a first processing submodule configured to perform a hash operation based on the hash key and the authentication image to obtain the password to be verified.

10. The apparatus of claim 8, further comprising an initializing module configured to set the verification password before receiving the authentication image.

11. The apparatus of claim 10, wherein the initializing module comprises:

a second acquiring submodule configured to acquire a password image selected by the user;

a generating submodule configured to generate a random number as a hash key; and

a second processing submodule configured to perform a hash operation according to the hash key and the password image to obtain the verification password.

12. The apparatus of claim 8, further comprising a display module configured to display a plurality of selectable authentication images on a display of a terminal device before the receiving module receives the authentication image selected by the user.

13. The apparatus of claim 8, further comprising a resetting module configured to: after obtaining the user identity authentication result, reset the verification password if user identity authentication is passed.

14. The apparatus of claim 8, wherein the verification module is further configured to authenticate the user according to a preset character string and reset the verification password after authentication is passed.

15. A non-transitory computer-readable storage medium having stored therein instructions that, when executed by a processor in a device, cause the device to perform operations including:

receiving an authentication image selected by a user;

acquiring, based on the authentication image, a password to be verified;

acquiring a preset verification password; and

comparing the verification password with the password to be verified to obtain a user identity authentication result.

16. The non-transitory computer-readable storage medium of claim 15, wherein acquiring the password to be verified comprises:

acquiring a pre-stored hash key; and

performing a hash operation based on the hash key and the authentication image to obtain the password to be verified.

17. The non-transitory computer-readable storage medium of claim 15, wherein the operations further comprise setting the verification password before receiving the authentication image.

18. The non-transitory computer-readable storage medium of claim 17, wherein setting the verification password comprises:

acquiring a password image selected by the user;

generating a random number as a hash key; and

performing a hash operation according to the hash key and the password image to obtain the verification password.

19. The non-transitory computer-readable storage medium of claim 15, wherein the operations further comprise:

after obtaining the user identity authentication result, resetting the verification password if user identity authentication is passed.

20. The non-transitory computer-readable storage medium of claim 15, wherein

the operations further comprise:

authenticating the user according to a preset character string; and

resetting the verification password after authentication is passed.

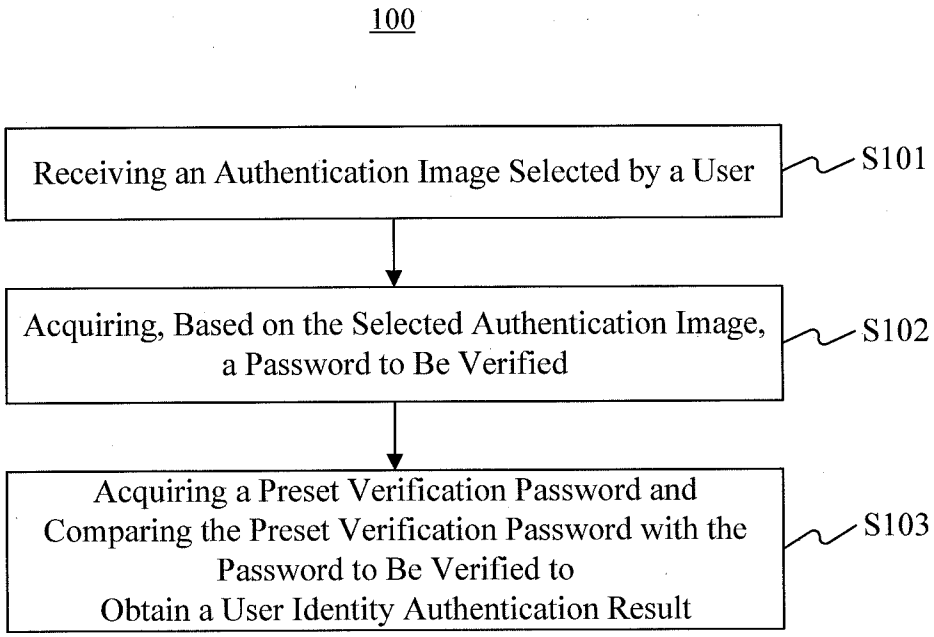
100
Receiving an Authentication Image Selected by a User
S101
Acquiring, Based on the Selected Authentication Image, a Password to Be Verified
S102
Acquiring a Preset Verification Password and Comparing the Preset Verification Password with the Password to Be Verified to Obtain a User Identity Authentication Result
S103

Fig. 1

200

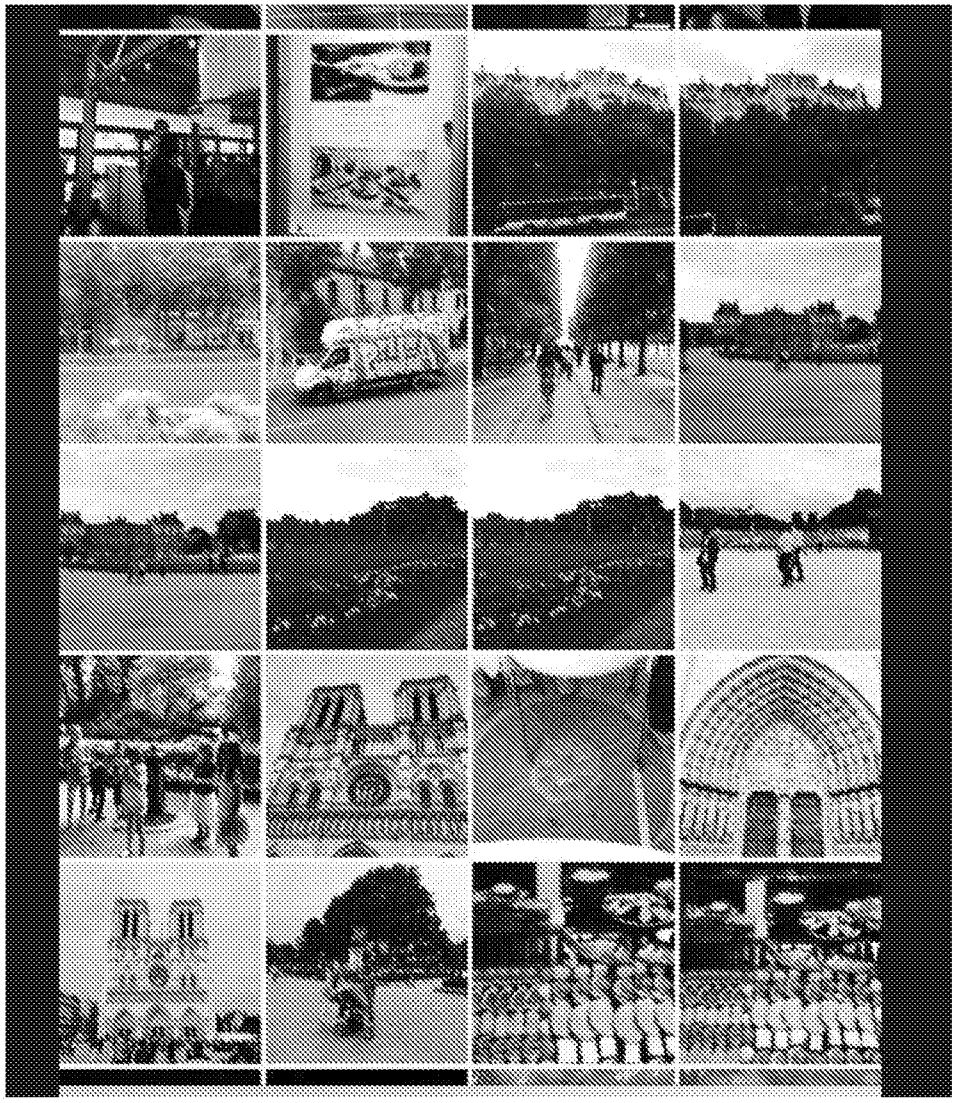

Fig. 2

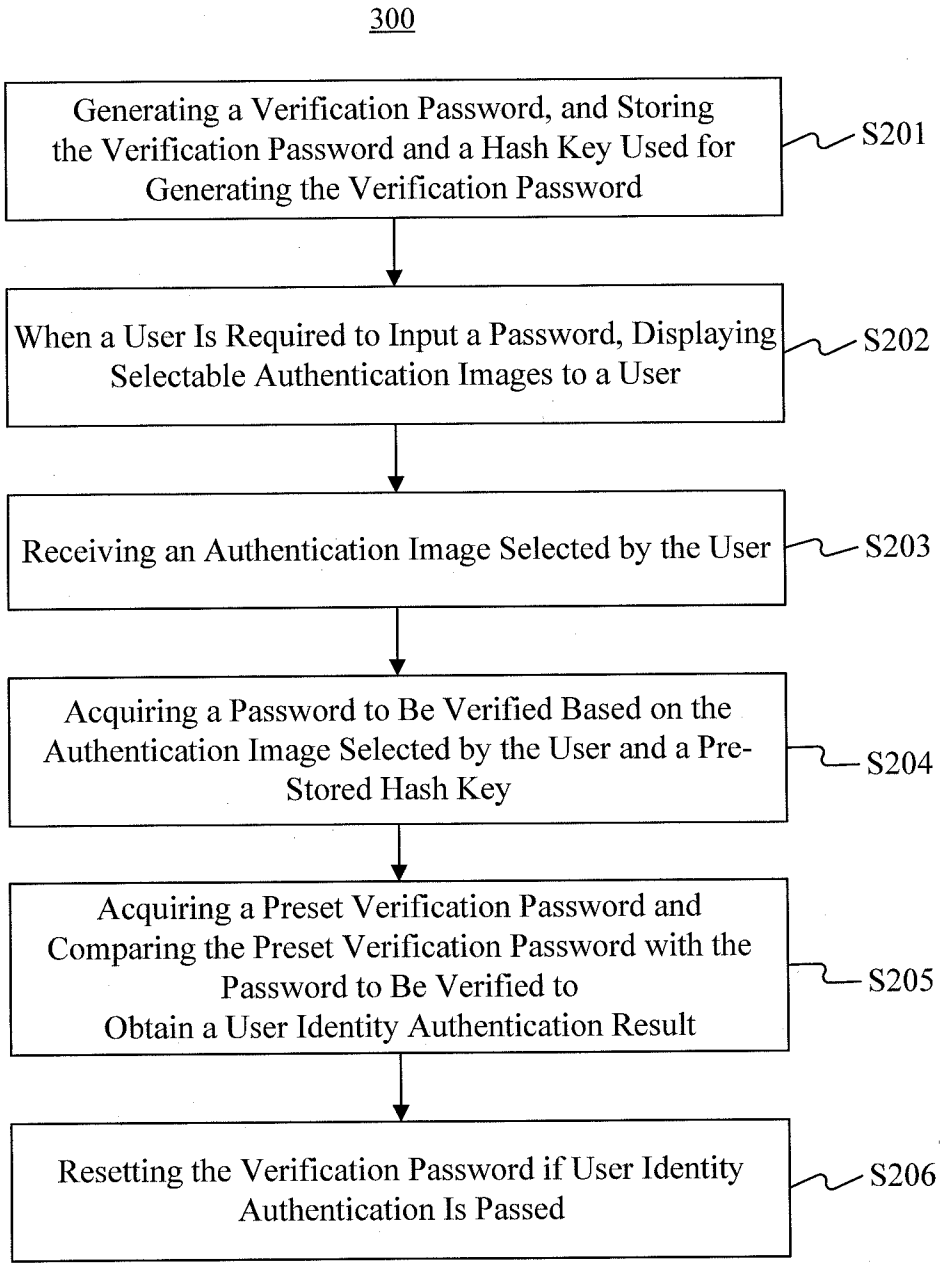
300
Generating a Verification Password, and Storing the Verification Password and a Hash Key Used for Generating the Verification Password
S201
When a User Is Required to Input a Password, Displaying Selectable Authentication Images to a User
S202
Receiving an Authentication Image Selected by the User
S203
Acquiring a Password to Be Verified Based on the Authentication Image Selected by the User and a Pre-Stored Hash Key
S204
Acquiring a Preset Verification Password and Comparing the Preset Verification Password with the Password to Be Verified to Obtain a User Identity Authentication Result
S205
Resetting the Verification Password if User Identity Authentication Is Passed
S206

Fig. 3

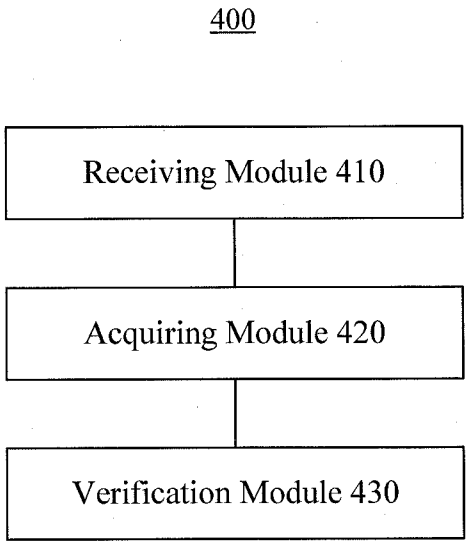
400
Receiving Module 410
Acquiring Module 420
Verification Module 430

Fig. 4

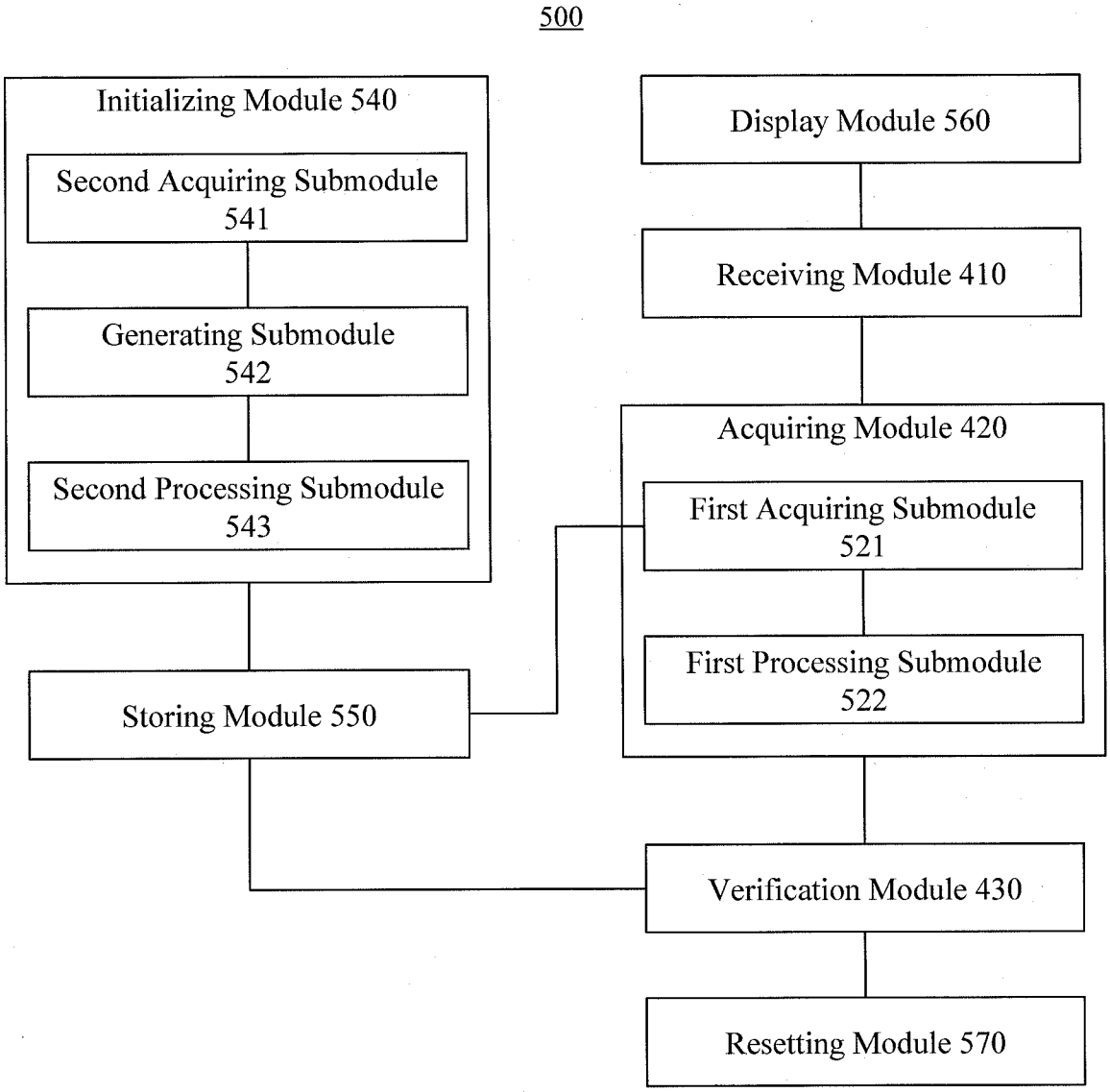
500
Initializing Module 540
Second Acquiring Submodule 541
Generating Submodule 542
Second Processing Submodule 543
Storing Module 550
Display Module 560
Receiving Module 410
Acquiring Module 420
First Acquiring Submodule 521
First Processing Submodule 522
Verification Module 430
Resetting Module 570

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US16/20214

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 21/36; H04L 9/08, 9/32 (2016.01)
CPC - G06F 21/36; H04L 9/0863, 9/3228
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G06F 21/36; H04L 9/08, 9/32 (2016.01)
CPC - G06F 21/36; H04L 9/0863, 9/3228, 63/12

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)
PatSeer (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, RU, AT, CH, TH, BR, PH, SE, NO, DK, FI, BE, NL, LU, Other Countries (INPADOC)); EBSCO; IEEE/IEEEXplore; Google/Google Scholar; Keywords: password, passcode, hash, encode, number, key, image, graphic, picture

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	EP 2254071 A1 (THOMSON LICENSING) 24 November 2010; Abstract; Paragraphs [0012], [0018], [0023], [0030], [0032], [0035], [0038], [0045]	1-5, 8-12, 15-18 --- 6, 7, 13, 14, 19, 20
Y	US 2007/0050635 A1 (POPP, N.) 1 March 2007; Paragraphs [0004], [0007], [0009], [0011]	6, 7, 13, 14, 19, 20
A	US 2004/0230843 A1 (JANSEN, W.) 18 November 2004; Entire Document	1-20
A	US 2012/0171997 A1 (KNAPP, R.) 5 July 2012; Entire Document	1-20

☐ 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
24 April 2016 (24.04.2016)	05 MAY 2016
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)