



(51) International Patent Classification:
G06F 21/32 (2013.01)

(21) International Application Number:
PCT/CN2021/107818

(22) International Filing Date:
22 July 2021 (22.07.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
202010720845.3 24 July 2020 (24.07.2020) CN

(71) Applicant (*for all designated States except CN*): **GIESECKE+DEVRIENT MOBILE SECURITY GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 Munich (DE).

(71) Applicant (*for CN only*): **GIESECKE+DEVRIENT (CHINA) TECHNOLOGIES CO., LTD.** [CN/CN]; 399 Huoju Avenue, Nanchang High-New Tech Development Zone, Nanchang, Jiangxi 330000 (CN).

(72) Inventors: **SUN, Guang**; Suite 902, Evergrande Plaza, 99 Tidu Street, Qingyang District, Chengdu, Sichuan 610015 (CN). **YUAN, Yubo**; Suite 902, Evergrande Plaza, 99 Tidu Street, Qingyang District, Chengdu, Sichuan 610015 (CN). **ZHANG, Tengyu**; Suite 902, Evergrande Plaza, 99 Tidu Street, Qingyang District, Chengdu, Sichuan 610015 (CN).

(74) Agent: **LIU, SHEN & ASSOCIATES**; 10th Floor, Building 1, 10 Caihefang Road, Haidian District, Beijing 100080 (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,

(54) Title: IDENTITY AUTHENTICATION METHOD, APPARATUS, DEVICES AND STORAGE MEDIA

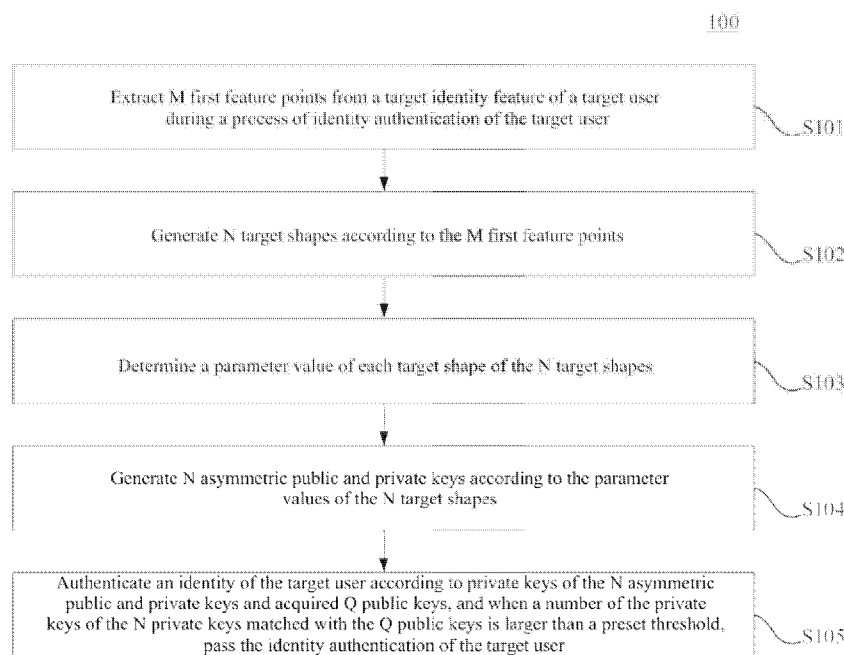


Fig. 1

(57) Abstract: The invention discloses an identity authentication method, apparatus, device and storage medium. the method comprises extracting M first feature points from a target identity feature of a target user; generating N target shapes according to the M first feature points; determining a parameter value of each target shape of the N target shapes; generating N asymmetric public and private keys according to the parameter values of the N target shapes; and authenticating an identity of the target user according to private keys in the N asymmetric public and private keys and acquired Q public keys, and when a number of the private keys of the N private keys matched with the Q public keys is larger than a preset threshold, passing the identity authentication of the target user; wherein the public keys are public key of the asymmetric public and private key generated according to parameter values of target shapes; and the parameter values of the target shapes are determined by W second feature points in the target identity feature of the target user. According to the

CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

IDENTITY AUTHENTICATION METHOD, APPARATUS, DEVICES AND STORAGE MEDIA

TECHNICAL FIELD

5 [0001] The invention belongs to the field of data security, and in particular, relates to an identity authentication method, apparatus, device and storage medium.

BACKGROUND

10 [0002] With the development of science and technology, in order to ensure the security of data stored in electronic devices, users must pass identity authentication before operating the electronic devices.

[0003] In related technologies, the electronic devices usually store the user's identity feature information in advance, and during identity authentication, it authenticates whether the input identity feature information matches the pre-stored identity feature information. When the input
15 identity feature information matches the pre-stored identity feature information, the identity authentication is passed. However, in this identity authentication method, the pre-stored user identity feature information is at risk of being lost or leaked. Therefore, this identity authentication method does not have high security.

SUMMARY

20 [0004] Embodiments of the present invention provide an identity authentication method, apparatus, device and storage medium, which can avoid the loss or leakage of user identity feature information and improve the security of an identity authentication mode.

[0005] In a first aspect, an identity authentication method is provided, which includes the
25 following steps:

[0006] extracting M first feature points from a target identity feature of a target user during a process of identity authentication of the target user;

[0007] generating N target shapes according to the M first feature points;

[0008] determining a parameter value of each target shape of the N target shapes;

30 [0009] generating N asymmetric public and private keys according to the parameter values of the N target shapes; and

[0010] authenticating an identity of the target user according to private keys of the N asymmetric public and private keys and acquired Q public keys, and when a number of the private keys of the N private keys matched with the Q public keys is larger than a preset threshold, passing the
35 identity authentication of the target user;

[0011] wherein the public keys are public keys of the asymmetric public and private key

generated according to parameter values of target shapes; and the parameter values of the target shapes are determined by W second feature points in the target identity feature of the target user; and

[0012] wherein M, N, Q and W are positive integers.

5 [0013] In a possible implementation, the authenticating an identity of the target user according to private keys of the N asymmetric public and private keys and acquired Q public keys, and when a number of the private keys of the N private keys matched with the Q public keys is larger than a preset threshold, passing the identity authentication of the target user specifically comprises the following steps:

10 [0014] using a private key of each asymmetric public and private key to sign an acquired random number so as to obtain N pieces of signature information; and

[0015] authenticating the N pieces of signature information by using the acquired Q public keys, and when a number of the N pieces of signature information matched with the Q public keys is larger than a preset threshold, passing the identity authentication of the target user.

15 [0016] In a possible implementation, before extracting M first feature points from the target identity feature of the target user, the method further comprises the following steps:

[0017] dividing the target identity feature into regions to obtain I regions;

[0018] extracting W second feature points from each of the I regions respectively;

20 [0019] for each region, generating P target shapes according to second feature points of each region;

[0020] calculating a parameter value of each target shape; and

[0021] generating Q asymmetric public and private keys according to the parameter value of each target shape to obtain the Q public keys;

[0022] In a possible implementation, the target shape is a triangle;

25 [0023] a relationship between M and N satisfies the following formula:

$$N = \frac{M \times (M - 1) \times (M - 2)}{6}$$

[0024]

[0025] a relationship between P and W satisfies the following formula:

$$P = \frac{W \times (W - 1) \times (W - 2)}{6}$$

[0026]

[0027] a relationship among I, P and Q satisfies the following formula:

30 [0028] $Q = I \cdot P$, and

[0029] wherein Q is greater than N.

[0030] In a possible implementation, the authenticating the N pieces of signature information by using the acquired Q public keys comprises the following steps:

[0031] performing the following steps for the Q public keys sequentially:

[0032] matching a public key with respective signature information in a signature set respectively; wherein the signature set is a set composed of the N pieces of signature information; and

[0033] when the public key matches a target signature information, removing the target signature information from the signature set to obtain an updated signature set; wherein the target signature information is any information in the signature set.

[0034] In a possible implementation, the parameter value of the target shape is a value of the circumference or a value of the area.

[0035] In a possible implementation, the target identity feature includes one of the following items: fingerprint feature, facial feature, palmprint feature.

[0036] In a second aspect, an identity authentication apparatus is provided, the identity authentication apparatus includes the following modules:

[0037] an extraction module, which is configured to extract M first feature points from a target identity feature of a target user during a process of identity authentication of the target user;

[0038] a generation module, which is configured to generate N target shapes according to the M first feature points;

[0039] a determination module, which is configured to determine a parameter value of each target shape of the N target shapes;

[0040] the generation module, which is further configured to generate N asymmetric public and private keys according to the parameter values of the N target shapes; and

[0041] an authentication module, which is configured to authenticate an identity of the target user according to private keys of the N asymmetric public and private keys and acquired Q public keys, and when a number of the private keys of the N private keys matched with the Q public keys is larger than a preset threshold, pass the identity authentication of the target user;

[0042] wherein the public keys are public keys of the asymmetric public and private key generated according to parameter values of target shapes; and the parameter values of the target shapes are determined by W second feature points in the target identity feature of the target user; and

[0043] wherein M, N, Q and W are positive integers.

[0044] In a possible implementation, the authentication module is specifically configured to perform the following steps:

[0045] using a private key of each asymmetric public and private key to sign an acquired random number so as to obtain N pieces of signature information; and

[0046] authenticating the N pieces of signature information by using the acquired Q public keys, and when a number of the N pieces of signature information matched with the Q public keys is

larger than a preset threshold, passing the identity authentication of the target user.

[0047] In a possible implementation, the apparatus further includes the following modules:

[0048] a division module, which is configured to divide the target identity feature into regions to obtain I regions;

5 [0049] an extraction module, which is configured to extract W second feature points from each of the I regions respectively;

[0050] the generation module, which is also configured to generate Q target shapes for each region according to the second feature point of each region;

[0051] a calculation module, which is configured to calculate a parameter value of each target
10 shape; and

[0052] the generation module, which is configured to generate Q asymmetric public and private keys according to the parameter value of each target shape to obtain the Q public keys.

[0053] In a possible implementation, the target shape is a triangle;

[0054] a relationship between M and N satisfies the following formula:

$$15 \quad [0055] \quad N = \frac{M \times (M-1) \times (M-2)}{6}$$

[0056] a relationship between I, Q and W satisfies the following formula:

$$[0057] \quad Q = I \cdot \frac{W \times (W-1) \times (W-2)}{6}, \text{ and}$$

[0058] wherein, Q is greater than N, and I are all positive integers.

[0059] In a possible implementation, the authentication module is specifically configured to
20 perform the following steps:

[0060] performing the following steps for the Q public keys sequentially:

[0061] matching the public key with respective signature information in a signature set respectively; wherein the signature set is a set composed of the N pieces of signature information; and

25 [0062] when the public key matches a target signature information, removing the target signature information from the signature set to obtain an updated signature set; wherein the target signature information is any information in the signature set.

[0063] In a possible implementation, the parameter value of the target shape is a value of the circumference or a value of the area.

30 [0064] In a possible implementation, the target identity feature comprises one of the following items: fingerprint feature, facial feature and palmprint feature.

[0065] In a third aspect, an electronic device is provided, the device comprises a processor and a memory storing computer program instructions; and when the processor executes the computer program instructions, the method as in the first aspect or any possible implementation of the first

aspect is implemented.

[0066] In a fourth aspect, a computer storage medium is provided. The computer storage medium stores computer program instructions. When the computer program instructions are executed by a processor, the method in the first aspect or any possible implementation of the first aspect is implemented.

[0067] Based on the provided identity authentication method, apparatus, device and storage medium, during a process of identity authentication of a target user, based on M first feature points extracted from a target identity feature of the target user, parameter values of feature parameters of N target shapes can be generated, and then asymmetric public and private keys can be generated based on the parameter values. The target user is authenticated based on private keys of the asymmetric public and private keys and acquired Q public keys. And an identity of the user is authenticated according to a plurality of feature points of the target identity feature input by the user. When a number of private keys of N private keys matched with the Q public keys is greater than a preset threshold, the identity authentication of the target user is passed.

Herein, the public keys are public keys of the asymmetric public and private key generated according to parameter values of target shapes; and the parameter values of the target shapes are determined by W second feature points in the target identity feature of the target user. As a result, the electronic device converts the user's identity feature information, such as facial feature, fingerprint feature, palmprint feature, etc., into digital representation, that is, the electronic device can authenticate the user's identity only by saving the public keys, without saving the original data of the user's identity features, thereby avoiding the loss or leakage of the user's identity information and improving the security of the identity authentication method.

BRIEF DESCRIPTION OF THE DRAWINGS

[0068] In order to explain the technical solutions of the embodiments of the present invention more clearly, the following will briefly introduce the drawings needed in the embodiments of the present invention. For those of ordinary skill in the art, other drawings can be obtained according to these drawings without paying creative labor.

[0069] Fig. 1 is a schematic flowchart of an identity authentication method provided by an embodiment of the present invention;

[0070] Fig. 2 is a schematic structural diagram of an identity authentication apparatus provided by an embodiment of the present invention; and

[0071] Fig. 3 is a schematic structural diagram of an electronic device provided by an embodiment of the present invention.

DETAILED DESCRIPTION

[0072] The features and exemplary embodiments of various aspects of the present invention will be described in detail below. In order to make the object, technical scheme and advantages of the present invention clearer, the present invention will be further described in detail with reference to the drawings and specific embodiments. It should be understood that the specific embodiments described herein are only configured to explain the present invention, and are not configured to limit the present invention. It will be apparent to those skilled in the art that the present invention may be practiced without some of these specific details. The following description of the embodiments is only for providing a better understanding of the present invention by illustrating examples of the present invention.

[0073] It should be noted that in this document, relational terms such as first and second are only used to distinguish one entity or operation from another entity or operation, and do not necessarily require or imply any such actual relationship or order between these entities or operations. Furthermore, the terms "including", "comprising" or any other variation thereof are intended to cover non-exclusive inclusion, so that a process, method, article or device including a series of elements includes not only those elements, but also other elements not explicitly listed, or elements inherent to such process, method, article or device. Without further restrictions, the elements defined by the sentence "including..." do not exclude the existence of other identical elements in the process, method, article or device including the elements.

[0074] With the development of science and technology, in order to ensure the security of data stored in electronic devices, users must pass identity authentication before operating the electronic devices.

[0075] In related technologies, the electronic devices usually store the user's identity feature information in advance, and during a process of identity authentication, they authenticate whether input identity feature information matches pre-saved identity feature information. When the input identity feature information is matched with the pre-saved identity feature information, the identity authentication is passed. For example, when a user uses a fingerprint for identity authentication, a pre-stored user fingerprint template is used in related technologies to match the user fingerprint entered into the electronic device. The fingerprint template saves complete data of the user's fingerprint, but in the case of data leakage of the electronic device, it is easy to leak the complete data of the user's fingerprint, which will cause unnecessary loss to the user after the complete data of the user's fingerprint are used by criminals. Therefore, in the identity authentication methods in related technologies, the pre-stored user identity feature information is at risk of being lost or leaked. Therefore, this identity authentication method does not have high security.

[0076] In addition, in related technologies, during the process of identity authentication, it is necessary to translate, rotate, scale and other transformations of a fingerprint saved in electronic devices, so as to complete the identity authentication. However, the translation, rotation and scaling of the fingerprint reduce the efficiency of identity authentication of electronic devices.

5 [0077] In order to solve the technical problems in related technologies, the embodiment of the present invention provides an identity authentication method, apparatus, device and storage medium, which can avoid the loss or leakage of user identity feature information and improve the security of the identity authentication mode.

10 [0078] In order to facilitate understanding of the embodiments of the present invention, the identity authentication method provided by the embodiments of the present invention is described in detail below.

[0079] Fig. 1 shows a schematic flowchart of an identity authentication method 100 provided by an embodiment of the present invention. As shown in Fig. 1, the identity authentication method 100 provided by the embodiment of the present invention may include the following steps.

15 [0080] At S101, M first feature points are extracted from a target identity feature of a target user during a process of identity authentication of the target user.

[0081] Before authenticating the user's identify, it is necessary to extract feature points of the user's identity feature, so as to complete the identity authentication of the user. The target user is a user who needs to be authenticated. For example, a target user A needs to use an application A in an electronic device to perform transfer operation, and the identity authentication of the target user A needs to be performed before perform the identity transfer, so the feature points of the identity features of the target user A need to be extracted. The target identity feature refers to any identity feature that can represent the user's identity. For example, the target identity feature may include fingerprint feature, facial feature and palmprint feature.

25 [0082] Before the user performs identity authentication, the electronic device needs to enter the user's target identity feature, and then the electronic device extracts M first feature points from the user's target identity feature. For example, if the user uses the user's facial feature for identity authentication, the user can use a camera device of the electronic device to photograph his own facial feature, so that the electronic device can extract feature points in the user's facial feature, and then authenticate the user.

[0083] As an example, the user A uses his fingerprint feature for identity authentication, and the user A transmits the fingerprint feature of the user A to the electronic device through a fingerprint entry module on the electronic device. After receiving the fingerprint feature of the user A, the electronic device extracts M feature points from the fingerprint feature.

35 [0084] At S102, N target shapes are generated according to the M first feature points.

[0085] Based on the extracted M first feature points, N target shapes are constructed. The M first feature points are connected to construct the N target shapes.

[0086] Here, the target shape may be a triangle.

[0087] Optionally, when the target shape is a triangle, a relationship between M and N satisfies the following formula (1):

$$N = \frac{M \times (M - 1) \times (M - 2)}{6} \quad (1)$$

[0088]

[0089] Here M and N are both positive integers.

[0090] In addition, the target shape may also be a polygon such as a quadrilateral. After the M first feature points are extracted, the M first feature points are connected to construct multiple polygons.

[0091] At S103, a parameter value of each target shape in the N target shapes is determined.

[0092] After the target shape is obtained, the parameter value of the target shape is calculated. Herein the parameter value may be a value of a perimeter or a value of an area. For example, if the target shape is a triangle, the parameter value may be a value of the perimeter of the triangle or a value of the area of the triangle.

[0093] At S104, N asymmetric public and private keys are generated according to the parameter values of the N target shapes.

[0094] Based on a parameter value of each target shape, asymmetric public and private keys corresponding to the parameter value is calculated. Thus, according to the parameter values of the N target shapes, N asymmetric public and private keys can be obtained.

[0095] At S105, an identity of the target user is authenticated according to private keys of the N asymmetric public and private keys and acquired Q public keys, and when a number of the private keys of the N private keys matched with the Q public keys is greater than a preset threshold, the identity authentication of the target user is passed.

[0096] The private keys of the N asymmetric public and private keys are matched with the acquired Q public keys, and when a number of the private keys of the N private keys matched with the Q public keys is greater than the preset threshold, the identity authentication of the target user is passed.

[0097] The Q public keys may be multiple public keys generated in advance and saved in the electronic device. The public keys are public key of the asymmetric public and private keys generated according to parameter values of a target shapes; and the parameter values of the target shapes are determined by the W second feature points in the target identity feature of the target user.

[0098] Optionally, in an embodiment of the present invention, before S101, the embodiment of the present invention may include the following steps.

[0099] The target identity feature is divided into regions to obtain I regions.

[00100] W second feature points are extracted from each of the I regions respectively.

[00101] For each region, P target shapes are generated according to the second feature points of each region.

5 [00102] A parameter value of each target shape is calculated.

[00103] According to the parameter value of each target shape, Q asymmetric public and private keys are generated, and Q public keys are obtained.

[00104] The user needs to save the identity feature in the electronic device. In order to ensure that the identity feature of the user is not leaked, the target identity feature needs to be divided
10 into regions to obtain I regions. For example, the fingerprint feature of the user is divided into 5 regions.

[00105] After the target identity feature is divided into regions, W second feature points are extracted from each region. The W second feature points of each region are connected to construct P target shapes. The parameter value of each target shape is calculated. The parameter
15 value may include a value of the perimeter of the target shape, a value of the area of the target shape, and the like. For example, the shape of the target is a triangle, and after P triangles are determined, the perimeter of each triangle is calculated. When the target shape is a triangle, the parameter value may also be a combination of angles, for example, three angles of the triangle are 90°, 45°, and 45°.

20 [00106] Optionally, when the target shape is a triangle, a relationship between P and W satisfies the following formula (2):

$$P = \frac{W \times (W - 1) \times (W - 2)}{6} \quad (2)$$

[00107]

[00108] Both P and W are positive integers.

[00109] A relationship between I, P, and Q satisfies the following formula (3):

25 [00110] $Q = I \cdot P$ (3).

[00111] Here I is a positive integer, and Q is greater than N.

[00112] Q asymmetric public and private keys are generated based on the parameter value of each target shape, and then Q public keys are obtained. Here, In order to ensure the security of information, after Q asymmetric public and private keys are generated, the private keys of the Q
30 asymmetric public and private keys may also be destroyed.

[00113] As a result, completion information of the user's target identity feature is converted into a digital form and saved in the electronic device, so that the user's identity authentication can be realized, the loss or leakage of the user's identity feature information can be avoided, and the security of the identity authentication mode can be improved.

[00114] Optionally, S105 in the identity authentication method 100 provided in the embodiment of the present invention specifically authenticates the N pieces of signature information in the following manner.

[00115] A private key of each asymmetric public and private key is used to sign an acquired random number, so as to obtain N pieces of signature information; and

[00116] The N pieces of signature information are authenticated by using the acquired Q public keys, and when a number of the N pieces of signature information matched with the Q public keys is greater than a preset threshold, the identity authentication of the target user is passed.

[00117] The private keys of the N asymmetric public and private keys are used to sign the acquired random number, and then obtain N pieces of signature information. The N pieces of signature information are authenticated by using Q public keys.

[00118] Optionally, the following steps are performed for Q public keys sequentially:

[00119] matching a public key with respective signature information in a signature set respectively; herein the signature set is a set composed of the N pieces of signature information; and

[00120] when the public key matches a target signature information, removing the target signature information from the signature set to obtain an updated signature set; herein the target signature information is any information in the signature set.

[00121] Take N pieces of signature information as a signature set. For Q public keys, N pieces of signature information may be authenticated sequentially. In other words, the authenticated public key does not need to be authenticated again. After matching the public key with the respective signature information, it is determined that the target signature information in the signature set matches the public key, and then the target signature information is removed from the signature set to obtain an updated signature set. The target signature information is any signature information in the signature set.

[00122] For example, the public keys are {A B C D E F G H I J} respectively, and the signature set is {1 2 3 4 5 6 7}. The signature information is authenticated by using a public key A, where the public key A matches signature information 2, then the signature set is updated to {1 3 4 5 6 7}. The public key B is used to authenticate the signature information. Where the public key B matches the signature information 5, then the signature set is updated to {1 3 4 6 7}, and so on.

[00123] When a number of signature information matched with the public key is greater than a preset threshold, the identity authentication of the target user is passed.

[00124] The identity authentication method 100 provided by the embodiment of the present invention can generate the parameter values of the feature parameters of the N target shape based on the M first feature points extracted from the target identity feature of the target user, and then

generate asymmetric public and private keys based on the parameter values. The target user is authenticated based on private keys of the asymmetric public and private keys and the acquired Q public keys. And the user's identity is authenticated with multiple feature points of the target identity feature input by the user. When a number of private keys of the N private keys matched with Q public keys is greater than the preset threshold, the identity authentication of the target user is passed. Herein the public keys are the public keys of the asymmetric public and private keys generated according to the parameter values of the target shapes; and the parameter values of the target shapes are determined by the W second feature points in the target identity feature of the target user. As a result, the electronic device converts the user's identity feature information, such as facial feature, fingerprint feature, palmprint feature, etc., into digital representation, that is, the electronic device can authenticate the user's identity only by saving the public keys, without saving the original data of the user's identity features, thereby avoiding the loss or leakage of the user's identity information and improving the security of the identity authentication method.

[00125] Moreover, the user's identity features are saved in a form of numbers, without changing of the user's identity features, such as translation, rotation or scaling, which improves the efficiency of user identity authentication.

[00126] Based on the embodiment of the method 100 corresponding to Fig. 1, the embodiment of the present invention also provides an identity authentication apparatus. The identity authentication apparatus will be described in detail below.

[00127] Fig. 2 is a schematic structural diagram of an identity authentication apparatus 200 provided by an embodiment of the present invention. As shown in Fig. 2, the identity authentication apparatus 200 provided in the embodiment of the present invention may include an extraction module 201, a generation module 202, a determination module 203, and an authentication module 204.

[00128] The extraction module 201 is configured to extract M first feature points from a target identity feature of a target user during a process of identity authentication of the target user.

[00129] The generation module 202 is configured to generate N target shapes according to the M first feature points.

[00130] The determination module 203 is configured to determine a parameter value of each target shape in the N target shapes.

[00131] The generation module 202 is further configured to generate N asymmetric public and private keys according to the parameter value of each target shape.

[00132] The authentication module 204 is configured to authenticate an identity of the target user according to private keys of the N asymmetric public and private keys and acquired Q public

keys, and when a number of the private keys of the N private keys matched with the Q public keys is larger than a preset threshold, pass the identity authentication of the target user.

[00133] Herein, the public keys are public keys of the asymmetric public and private key generated according to parameter values of the target shapes; and the parameter values of the target shapes are determined by the W second feature points in the target identity feature of the target user.

[00134] Herein, M, N, Q, and W are positive integers.

[00135] In a possible implementation, the authentication module 204 is specifically configured to perform the following steps:

[00136] using a private key of each asymmetric public and private key to sign an acquired random number so as to obtain N pieces of signature information; and

[00137] authenticating the N pieces of signature information by using the acquired Q public keys, and when a number of the N pieces of signature information matched with the Q public keys is larger than a preset threshold, passing the identity authentication of the target user.

[00138] In a possible implementation, the apparatus further includes the following modules:

[00139] a division module 205, which is configured to divide the target identity feature into regions to obtain I regions;

[00140] an extraction module 206, which is further configured to extract W second feature points from each of the I regions respectively;

[00141] the generation module 202, which is further configured to generate Q target shapes for each region according to second feature points of each region;

[00142] a calculation module 207, which is configured to calculate a parameter value of each target shape; and

[00143] the generation module 202, which is further configured to generate Q asymmetric public and private keys according to the parameter value of each target shape, and obtain Q public keys.

[00144] In a possible implementation, the target shape is a triangle;

[00145] a relationship between M and N satisfies the following formula:

$$N = \frac{M \times (M-1) \times (M-2)}{6}$$

[00146]

[00147] a relationship between I, Q and W satisfies the following formula:

$$Q = I \cdot \frac{W \times (W-1) \times (W-2)}{6}$$

[00148], and

[00149] Herein, Q is greater than N, and I are all positive integers.

[00150] In a possible implementation, the authentication module 204 is specifically configured to perform the following steps:

[00151] performing the following steps for the Q public keys sequentially:

[00152] matching a public key with respective signature information in a signature set respectively; herein the signature set is a set composed of the N pieces of signature information; and

[00153] when the public key matches the target signature information, removing the target signature information from the signature set to obtain an updated signature set; herein the target signature information is any information in the signature set.

[00154] In a possible implementation, the parameter value of the target shape is a value of the circumference or a value of the area.

[00155] In a possible implementation, the target identity feature includes one of the following items: fingerprint feature, facial feature, palmprint feature.

[00156] The identity authentication apparatus 200 provided by the embodiment of the present invention performs various steps in the method 100 shown in Fig. 1, and can avoid the loss or leakage of the user identity feature information and improve the technical effect of the security of the identity authentication mode, and for the sake of concise description, it will not be described in detail here.

[00157] According to the identity authentication apparatus 200 provided by the embodiment of the present invention, parameter values of feature parameters of N target shapes can be generated based on M first feature points extracted from a target identity feature of a target user, and then asymmetric public and private keys can be generated based on the parameter values. The target user is authenticated based on private keys of the asymmetric public and private keys and acquired Q public keys. And an identity of the user is authenticated according to a plurality of feature points of the target identity feature input by the user. When a number of private keys of N private keys matched with the Q public keys is greater than the preset threshold, the identity authentication of the target user is passed. Herein, the public keys are public keys of the asymmetric public and private keys generated according to parameter values of target shapes; and the parameter values of the target shapes are determined by W second feature points in the target identity feature of the target user. As a result, the electronic device converts the user's identity feature information, such as facial feature, fingerprint feature, palmprint feature, etc., into digital representation, that is, the electronic device can authenticate the user's identity only by saving the public keys, without saving the original data of the user's identity features, thereby avoiding the loss or leakage of the user's identity information and improving the security of the identity authentication method.

[00158] Moreover, the user's identity features are saved in a form of numbers, without changing of the user's identity features, such as translation, rotation and scaling, which improves the efficiency of user identity authentication.

[00159] Fig. 3 shows a schematic diagram of the hardware structure of an electronic device provided by an embodiment of the present invention.

[00160] The electronic device may include a processor 301 and a memory 302 storing computer program instructions.

5 [00161] Specifically, the aforementioned processor 301 may include a central processing unit (CPU), or an Application Specific Integrated Circuit (ASIC), or may be configured as one or more integrated circuits for implementing the embodiments of the present invention.

[00162] The memory 302 may include a mass storage for data or instructions. By way of example and not limitation, the memory 302 may include a hard disk drive (Hard Disk Drive, HDD), a floppy disk drive, a flash memory, an optical disk, a magneto-optical disk, a magnetic tape or a universal serial bus (USB) drive, or a combination of two or more of these. Where appropriate, the memory 302 may include removable or non-removable (or fixed) media. Where appropriate, the memory 302 may be internal or external to the integrated gateway disaster tolerance device. In a particular embodiment, the memory 302 is a non-volatile solid-state memory.

[00163] The memory may include read-only memory (ROM), random access memory (RAM), magnetic disk storage media devices, optical storage media devices, flash memory devices, electrical, optical, or other physical/tangible memory storage devices. Therefore, generally, the memory includes one or more tangible (non-transitory) computer-readable storage media (e.g., memory devices) encoded with software including computer-executable instructions, and when the software is executed (e.g., by one or more processors), it is operable to execute the operations described with reference to the method according to an aspect of the present invention.

[00164] The processor 301 reads and executes the computer program instructions stored in the memory 302 to implement any one of the identity authentication methods in the foregoing embodiments.

[00165] In an example, the electronic device may further include a communication interface 303 and a bus 310. Herein, as shown in Fig. 3, the processor 301, the memory 302, and the communication interface 303 are connected through the bus 310 and complete mutual communication.

30 [00166] The communication interface 303 is mainly used to implement communication between various modules, apparatuses, units and/or devices in the embodiments of the present invention.

[00167] The bus 310 includes hardware, software, or both, and couples the components of the identity authentication device to each other. By way of example and not limitation, the bus may include accelerated graphics port (AGP) or other graphics bus, enhanced industry standard architecture (EISA) bus, front side bus (FSB), hyper transfer (HT) interconnect, industry

standard architecture (ISA) Bus, unlimited bandwidth interconnect, low pin count (LPC) bus, memory bus, microchannel architecture (MCA) bus, peripheral component interconnect (PCI) bus, PCI-Express (PCI-X) bus, serial advanced technology Attachment (SATA) bus, Video Electronics Standards Association Local (VLB) bus or other suitable bus or a combination of two or more of these. Where appropriate, the bus 310 may include one or more buses. Although the embodiments of the present invention describe and show a specific bus, the present invention contemplates any suitable bus or interconnection.

[00168] The electronic device can execute the identity authentication method in the embodiment of the present invention, thereby realizing the identity authentication method described in conjunction with Fig. 1 and the identity authentication apparatus described in Fig. 2.

[00169] In addition, in combination with the identity authentication method in the foregoing embodiment, the embodiment of the present invention may provide a computer storage medium for implementation. The computer storage medium stores computer program instructions; and when the computer program instructions are executed by the processor, any one of the identity authentication methods in the foregoing embodiments is implemented.

[00170] It should be clear that the present invention is not limited to the specific configuration and processing described above and shown in the drawings. For brevity, a detailed description of the known method is omitted here. In the above embodiment, several specific steps are described and shown as examples. However, the method process of the present invention is not limited to the specific steps described and shown, and those skilled in the art can make various changes, modifications and additions, or change the order between the steps after understanding the spirit of the present invention.

[00171] The functional blocks shown in the above-mentioned structural block diagram can be implemented as hardware, software, firmware, or a combination thereof. When implemented in hardware, it can be, for example, an electronic circuit, an application specific integrated circuit (ASIC), appropriate firmware, a plug-in, a function card, etc. When implemented in software, the elements of the present invention are programs or code segments used to perform required tasks. Programs or code segments can be stored in a machine-readable medium, or transmitted on a transmission medium or a communication link through a data signal carried in a carrier wave. "Machine-readable medium" can include any medium capable of storing or transmitting information. Examples of machine-readable media include electronic circuits, semiconductor memory devices, ROM, flash memory, erasable ROM (EROM), floppy disks, CD-ROMs, optical disks, hard disks, fiber optic media, radio frequency (RF) links, and so on. The code segment can be downloaded via a computer network such as the Internet, an intranet, etc.

[00172] It should also be noted that the exemplary embodiments mentioned in the present invention describe some methods or systems based on a series of steps or apparatuses. However, the present invention is not limited to the order of the above steps, that is, the steps may be performed in the order mentioned in the embodiments, or may be different from the order in the
5 embodiments, or several steps may be performed at the same time.

[00173] Aspects of the present invention have been described above with reference to the flowcharts and/or block diagrams of the methods, apparatuses (systems) and computer program products according to the embodiments of the present invention. It should be understood that each block in the flowcharts and/or block diagrams and combinations of blocks in the flowcharts
10 and/or block diagrams can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, a special purpose computer, or other programmable data processing apparatus to produce a machine such that the instructions, which are executed via the processor of the computer or other programmable data processing apparatus, enable the implementation of the functions/acts
15 specified in one or more blocks of the flowchart and/or block diagram. Such a processor can be, but is not limited to, a general-purpose processor, a special-purpose processor, an application-specific processor or a field programmable logic circuit. It can also be understood that each block in the block diagram and/or flowchart and combinations of blocks in the block diagram and/or flowchart can also be implemented by dedicated hardware that performs specified functions or
20 actions, or by combinations of dedicated hardware and computer instructions.

[00174] The above is only a specific embodiment of the present invention, and it can be clearly understood by those skilled in the art that for the convenience and conciseness of description, the specific working processes of the systems, modules and units described above can refer to the corresponding processes in the aforementioned method embodiments, and will not be
25 described in detail here. It should be understood that the protection scope of the present invention is not limited to this, and any person familiar with the technical field can easily think of various equivalent modifications or substitutions within the technical scope disclosed by the present invention, which should be covered within the protection scope of the present invention.

CLAIMS

1. An identity authentication method, comprising:

extracting M first feature points from a target identity feature of a target user during a process of identity authentication of the target user;

5 generating N target shapes according to the M first feature points;

determining a parameter value of each target shape of the N target shapes;

generating N asymmetric public and private keys according to the parameter values of the N target shapes; and

10 authenticating an identity of the target user according to private keys of the N asymmetric public and private keys and acquired Q public keys, and when a number of the private keys of the N private keys matched with the Q public keys is larger than a preset threshold, passing the identity authentication of the target user;

wherein the public keys are public keys of the asymmetric public and private key generated according to parameter values of target shapes; and the parameter values of the target shapes are
15 determined by W second feature points in the target identity feature of the target user; and

wherein M, N, Q and W are positive integers.

2. The method according to claim 1, wherein the authenticating an identity of the target user according to private keys of the N asymmetric public and private keys and acquired Q public
20 keys, and when a number of the private keys of the N private keys matched with the Q public keys is larger than a preset threshold, passing the identity authentication of the target user, specifically comprises:

using a private key of each asymmetric public and private key to sign an acquired random number so as to obtain N pieces of signature information; and

25 authenticating the N pieces of signature information by using the acquired Q public keys, and when a number of the N pieces of signature information matched with the Q public keys is larger than a preset threshold, passing the identity authentication of the target user.

3. The method according to claim 1, wherein before extracting M first feature points from
30 the target identity feature of the target user, the method further comprises:

dividing the target identity feature into regions to obtain I regions;

extracting W second feature points from each of the I regions respectively;

for each region, generating P target shapes according to second feature points of each region;

calculating a parameter value of each target shape; and

generating Q asymmetric public and private keys according to the parameter value of each target shape to obtain the Q public keys;
wherein I and P are positive integers.

- 5 4. The method according to claim 3, wherein the target shape is a triangle;
a relationship between M and N satisfies the following formula:

$$N = \frac{M \times (M-1) \times (M-2)}{6}$$

a relationship between P and W satisfies the following formula:

$$P = \frac{W \times (W-1) \times (W-2)}{6}$$

- 10 a relationship among I, P and Q satisfies the following formula:

$$Q = I \cdot P, \text{ and}$$

wherein Q is greater than N.

- 15 5. The method according to claim 1, wherein the authenticating the N pieces of signature information by using the acquired Q public keys comprises:

performing the following steps for the Q public keys sequentially:

matching a public key with respective signature information in a signature set respectively;

wherein the signature set is a set composed of the N pieces of signature information; and

- 20 when the public key matches a target signature information, removing the target signature information from the signature set to obtain an updated signature set; wherein the target signature information is any information in the signature set.

- 25 6. The method according to any one of claims 1-5, wherein the parameter value of the target shape is a value of perimeter or a value of area.

7. The method according to any one of claims 1-5, wherein the target identity feature comprises one of the following items: fingerprint feature, facial feature and palmprint feature.

- 30 8. An identity authentication apparatus, comprising:
an extraction module, configured to extract M first feature points from a target identity feature of a target user during a process of identity authentication of the target user;
a generation module, configured to generate N target shapes according to the M first feature points;

a determination module, configured to determine a parameter value of each target shape of the N target shapes;

the generation module, further configured to generate N asymmetric public and private keys according to the parameter values of the N target shapes; and

5 an authentication module, configured to authenticate an identity of the target user according to private keys of the N asymmetric public and private keys and acquired Q public keys, and when a number of the private keys of the N private keys matched with the Q public keys is larger than a preset threshold, passing the identity authentication of the target user;

10 wherein the public keys are public keys of the asymmetric public and private key generated according to parameter values of target shapes; and the parameter values of the target shapes are determined by W second feature points in the target identity feature of the target user; and wherein M, N, Q and W are positive integers.

15 9. An electronic device, comprising: a processor and a memory storing computer program instructions; wherein

when the processor executes the computer program instructions, the method according to any one of claims 1-7 is implemented.

20 10. A computer storage medium having stored thereon computer program instructions which, when executed by a processor, implement the method according to any one of claims 1-7.

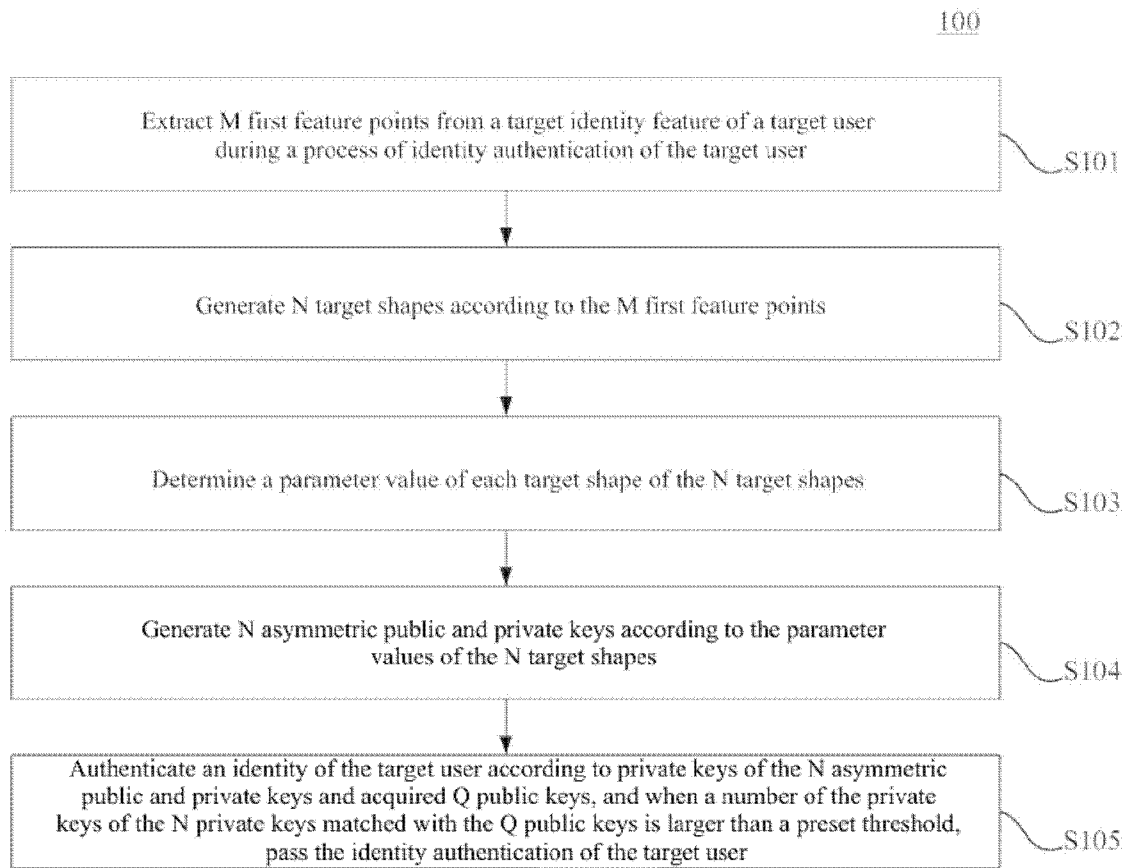


Fig. 1

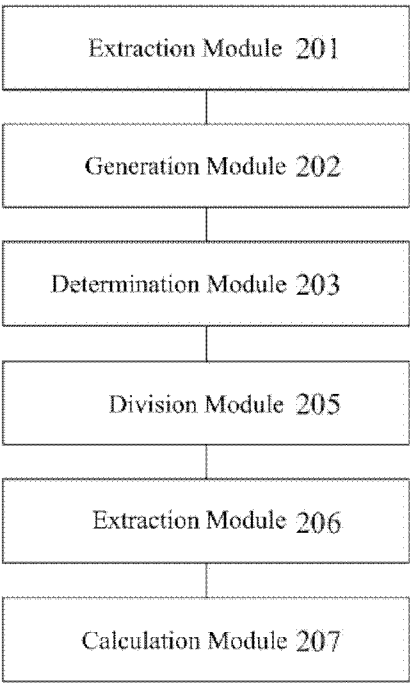


Fig. 2

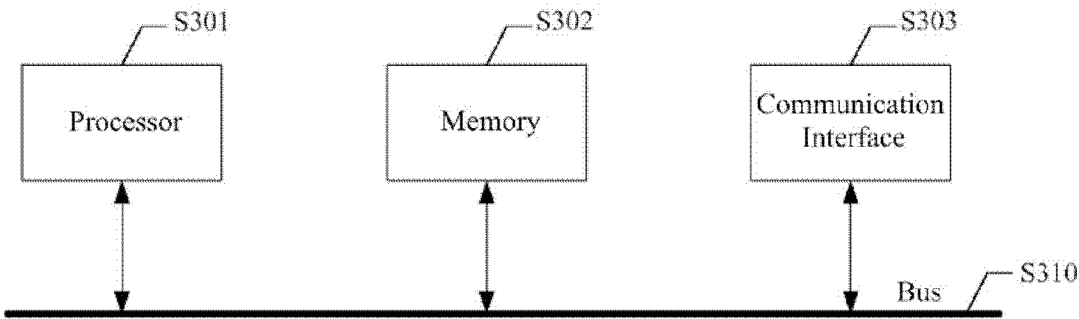


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/107818

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32(2013.01)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)

G06F

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)

SIPOABS; DWPI; CNABS; CNTXT; IEEE; CNKI: public key?, private key?, identity, authenticat+, feature?, parameter, fingerprint, face, shape

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 111931146 A (GIESECKE DEVRIENT CHINA TECH CO LTD) 13 November 2020 (2020-11-13) claims 1-10	1-10
Y	CN 110995410 A (HANGZHOU YUNCUI LIUTU NETWORK TECH CO LTD) 10 April 2020 (2020-04-10) abstract, claims 1-12, description pages 3-6	1-3, 5-10
Y	CN 101414903 A (XIANPING WU) 22 April 2009 (2009-04-22) abstract, claims 1-9, description pages 3-6	1-3, 5-10
A	US 2016071101 A1 (WINARSKI TYSON YORK) 10 March 2016 (2016-03-10) the whole document	1-10
A	CN 108650266 A (PING AN TECH SHENZHEN CO LTD) 12 October 2018 (2018-10-12) the whole document	1-10



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

18 October 2021

Date of mailing of the international search report

01 November 2021

Name and mailing address of the ISA/CN

National Intellectual Property Administration, PRC
6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088
China

Authorized officer

LIU, Huan

Facsimile No. (86-10)62019451

Telephone No. 86-010-62411658

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/107818

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	111931146	A	13 November 2020	None			
CN	110995410	A	10 April 2020	None			
CN	101414903	A	22 April 2009	CN	101414903	B	21 December 2011
				HK	1131846	A1	24 August 2012
US	2016071101	A1	10 March 2016	None			
CN	108650266	A	12 October 2018	WO	2019218512	A1	21 November 2019
				CN	108650266	B	18 February 2020