

**AUTHENTICATION AND AUTHENTICATION MODE DETERMINATION METHOD,
APPARATUS, AND ELECTRONIC DEVICE**

Cross-Reference to Related Applications

5 [0001] This application is based upon and claims priority to Chinese Patent Application No. 201811050088.2, filed on September 10, 2018, the entire content of all of which is incorporated herein by reference.

Technical Field

10 [0002] This application relates to the field of computer technologies, and in particular, to an authentication and authentication mode determination method, apparatus and electronic device.

Background

15 [0003] With the continuous development of pattern recognition and artificial intelligence technologies, the face recognition technology has been more and more widely applied. At present, face scan payment based on the face recognition technology has been gradually applied to people's daily life.

20 [0004] Face scan payment can use a human face feature as a password, thus eliminating the need for manually inputting a password and greatly simplifying an electronic payment process of a user. However, for users of multiple births, due to the great similarity of their face features, it is difficult for face scan payment to simply carry out identity recognition based on face features. Multiple births include two or more persons born in one pregnancy such as twins and triplets.

25 [0005] Therefore, when users of multiple births use face scan payment, it is still necessary to provide a further solution for how to identify such users.

Summary of the Invention

[0006] An authentication and authentication mode determination method, apparatus and electronic device are provided in embodiments of this application to solve the problem in the prior art that users of multiple births cannot be identified based on face features.

5 [0007] In order to solve the foregoing technical problem, the embodiments of this application are implemented as follows.

[0008] In a first aspect, an authentication method is provided, comprising: acquiring a front face feature and a side face feature of a user in response to a face authentication request of the user; searching, based on the front face feature and the side face feature of the user, a list of multiple
10 births corresponding to the user for a candidate user matching both the front face feature and the side face feature of the user, wherein the list of multiple births corresponding to the user is a list of multiple births with similar front face features and non-similar side face features; and determining, based on consistency between the candidate user and the user in the front face feature and the side face feature, whether the user succeeds in the authentication.

15 [0009] In a second aspect, an authentication mode determination method is provided, comprising: acquiring user information of a user in response to a request for activating a face authentication mode from the user; and determining an authentication mode for the user based on first user information with similar front face features and non-similar side face features in a list of multiple births, second user information with similar front face features and similar side face
20 features in the list of multiple births, and the user information of the user.

[0010] In a third aspect, an authentication apparatus is provided, comprising: an acquisition unit configured to acquire a front face feature and a side face feature of a user in response to a face authentication request of the user; a searching unit configured to search, based on the front face feature and the side face feature of the user, a list of multiple births corresponding to the user for a
25 candidate user matching both the front face feature and the side face feature of the user, wherein

the list of multiple births corresponding to the user is a list of multiple births with similar front face features and non-similar side face features; and a determination unit configured to determine, based on consistency between the candidate user and the user in the front face feature and the side face feature, whether the user succeeds in the authentication.

- 5 **[0011]** In a fourth aspect, an authentication mode determination apparatus is provided, comprising: an acquisition unit configured to acquire user information of a user in response to a request for activating a face authentication mode from the user; and a determination unit configured to determine an authentication mode for the user based on first user information with similar front face features and non-similar side face features in a list of multiple births, second user information
- 10 with similar front face features and similar side face features in the list of multiple births, and the user information of the user.

- [0012]** In a fifth aspect, an electronic device is provided, the electronic device comprising: a processor; and a memory configured to store a computer executable instruction, wherein when executed, the executable instruction causes the processor to perform the following operations:
- 15 acquiring a front face feature and a side face feature of a user in response to a face authentication request of the user; searching, based on the front face feature and the side face feature of the user, a list of multiple births corresponding to the user for a candidate user matching both the front face feature and the side face feature of the user, wherein the list of multiple births corresponding to the user is a list of multiple births with similar front face features and non-similar side face features;
- 20 and determining, based on consistency between the candidate user and the user in the front face feature and the side face feature, whether the user succeeds in the authentication.

- [0013]** In a sixth aspect, a computer readable storage medium is provided, wherein one or more programs are stored in the computer readable storage medium, and when executed by an electronic device that includes a plurality of applications, the one or more programs cause the
- 25 electronic device to perform the following operations: acquiring a front face feature and a side face

feature of a user in response to a face authentication request of the user; searching, based on the front face feature and the side face feature of the user, a list of multiple births corresponding to the user for a candidate user matching both the front face feature and the side face feature of the user, wherein the list of multiple births corresponding to the user is a list of multiple births with similar front face features and non-similar side face features; and determining, based on consistency between the candidate user and the user in the front face feature and the side face feature, whether the user succeeds in the authentication.

[0014] In a seventh aspect, an electronic device is provided, the electronic device comprising: a processor; and a memory configured to store a computer executable instruction, wherein when executed, the executable instruction causes the processor to perform the following operations: acquiring user information of a user in response to a request for activating a face authentication mode from the user; and determining an authentication mode for the user based on first user information with similar front face features and non-similar side face features in a list of multiple births, second user information with similar front face features and similar side face features in the list of multiple births, and the user information of the user.

[0015] In an eighth aspect, a computer readable storage medium is provided, wherein one or more programs are stored in the computer readable storage medium, and when executed by an electronic device that includes a plurality of applications, the one or more programs cause the electronic device to perform the following operations: acquiring user information of a user in response to a request for activating a face authentication mode from the user; and determining an authentication mode for the user based on first user information with similar front face features and non-similar side face features in a list of multiple births, second user information with similar front face features and similar side face features in the list of multiple births, and the user information of the user.

[0016] The foregoing technical solutions adopted in the embodiments of this application

can achieve at least the following technical effects.

[0017] A front face feature and a side face feature of a user are acquired in response to a face authentication request of the user, then a list of multiple births corresponding to the user is searched, based on the front face feature and the side face feature of the user, for a candidate user
5 matching both the front face feature and the side face feature of the user, wherein the list of multiple births corresponding to the user is a list of multiple births with similar front face features and non-similar side face features, and finally, it can be determined, based on consistency between the candidate user and the user in the front face feature and the side face feature, whether the user succeeds in the authentication. As such, when the authenticated user is a user of multiple births,
10 the front face feature and the side face feature of the user can be acquired and then compared with front face features and side face features of users in the pre-established list of multiple births to determine whether the user succeeds in the authentication, thus solving the problem of identifying using face features of a user of multiple births in the prior art.

[0018] User information of a user is acquired in response to a request for activating a face
15 authentication mode from the user, and then an authentication mode is determined for the user based on first user information with similar front face features and second user information with similar front face features and similar side face features in the list of multiple births, and the user information of the user. As such, when the user intended to activate the face authentication mode is a user of multiple births, a specific authentication mode can be determined for the user by
20 determining whether the user is a user only with a similar front face feature in the list of multiple births, a user with both a similar front face feature and a similar side face feature in the list of multiple births, or a user with a non-similar front face feature in the list of multiple births, so that some users in the list of multiple births can also activate a face authentication mode.

Brief Description of the Drawings

[0019] The accompanying drawings described here are used to provide further understanding of this application and form a part of this application. In the drawings,

[0020] FIG. 1 is a schematic diagram of an implementation process of an authentication
5 method according to an embodiment of this specification;

[0021] FIGS. 2(a) and 2(b) are schematic diagrams of a construction process of a list of multiple births according to an embodiment of this specification;

[0022] FIG. 3 is a schematic diagram of an implementation process of an authentication mode determination method according to an embodiment of this specification;

10 [0023] FIG. 4 is a schematic diagram of a process of determining an authentication mode applied to an actual scenario according to an embodiment of this specification;

[0024] FIG. 5 is a schematic structural diagram of an authentication apparatus according to an embodiment of this specification;

[0025] FIG. 6 is a schematic structural diagram of an authentication mode determination
15 apparatus according to an embodiment of this specification;

[0026] FIG. 7 is a schematic structural diagram of an electronic device according to an embodiment of this specification; and

[0027] FIG. 8 is a schematic structural diagram of another electronic device according to an embodiment of this specification.

20

Detailed Description

[0028] In order to make the objectives, technical solutions, and advantages of this application much clearer, the technical solutions of this application will be clearly and completely described in the following in combination with specific embodiments and the corresponding
25 accompanying drawings of this application. It is apparent that the embodiments described are

merely some of rather than all the embodiments of this application. All other embodiments obtained by those of ordinary skill in the art based on the embodiments in this application without creative efforts should be encompassed in the protection scope of this application.

[0029] The technical solutions provided in the embodiments of this application are
5 described in detail in the following with reference to the accompanying drawings.

[0030] In order to solve the problem in the prior art that users of multiple births cannot be identified based on face features, an authentication method and an authentication mode determination method are provided in the embodiments of this specification. The method provided in the embodiments of this specification may be executed by, but not limited to, a user terminal,
10 such as a mobile phone, a tablet computer, and a personal computer.

[0031] For ease of description, an implementation manner of the method is introduced in the following by taking that the method is performed by a terminal device capable of performing the method as an example. It should be appreciated that the method being performed by a terminal device is only an example description, which should not be construed as a limitation to the method.

[0032] Specifically, a schematic diagram of an implementation process of an authentication method according to one or more embodiments of this specification is shown in FIG. 1, including the following steps.

[0033] In step 110, a front face feature and a side face feature of a user are acquired in response to a face authentication request of the user.

[0034] Optionally, acquiring a front face feature and a side face feature of a user can specifically be: first determining whether the user is in a list of multiple births with similar front face features; and then acquiring the front face feature and the side face feature of the user if it is determined that the user is in the list of multiple births with similar front face features.

[0035] It should be appreciated that the multiple births in the embodiment of this application include two or more persons born in one pregnancy, for example, twins, triplets,
25

quadruplets, and so on. The multiple births mentioned below are similar to this, and will not be described in detail.

[0036] As users in the list of multiple births may not have the same front face features, for example, there are some differences in face features between fraternal twins, it can be determined whether the user is in the list of multiple births with similar front face features, and the front face feature and the side face feature of the user are acquired when it is determined that the user is in the list of multiple births with similar front face features.

[0037] It should be appreciated that whether the user is in the list of multiple births can be determined by acquiring a user ID and determining whether the user ID is in the list of multiple births. The user information included in the list of multiple births can specifically be user IDs, and each user ID corresponds to a unique user. In other words, the user ID is unique identification information of the user.

[0038] For users of multiple births, the similarity of their face features is often high. If face authentication is performed on the users with high similarity of face features, the result of authentication may be inaccurate. In order to avoid the problem of the inaccurate result of authentication caused by face authentication on the users of multiple births, in the prior art, a list of the users with high similarity of face features may be established in advance for the users of multiple births in combination with their identity information and the similarity of face features.

[0039] When the users with high similarity of face features, such as twins, want to activate or use a face authentication function, they are often prompted to use another authentication mode. In other words, in the prior art, the users with high similarity of face features are often forbidden from using the face authentication function to avoid the problem of the inaccurate result of authentication caused when the users use face authentication.

[0040] However, although the problem of the inaccurate result of authentication caused when the users use face authentication is avoided by forbidding the users with high similarity of

face features from using the face authentication function, some inconveniences are brought about to the users. That is, when the users perform operations requiring authentication such as payment, they need to perform authentication through some relatively cumbersome operations, such as entering a password. In one or more embodiments of this specification, in order to solve this
5 problem to enable users of multiple births to also use a face authentication mode, a list of multiple births is constructed in advance based on user information and similarities in face features of all users.

[0041] As shown in FIG. 2(a), it is a schematic diagram of a process of constructing a list of multiple births according to one or more embodiments of this specification, including the
10 following steps.

[0042] In step 21, a list of multiple births is acquired based on user information of all users.

[0043] By taking a payment application for payment as an example, user information of all users using the payment application, such as date of birth, registered permanent residence, residence and other information, can be acquired in advance to determine which users in all the
15 users using the payment application are users of multiple births, thus acquiring a list of multiple births. As shown in FIG. 2(b), the circle with the largest range in the figure is the list of multiple births acquired.

[0044] In step 22, front face features and side face features of users are acquired for each group of users of multiple births.

20 [0045] By continuing to take the foregoing payment application as an example, in order to improve the level of information security, avatar information of a user can be collected when the user registers the payment application. Specifically, a front face image and a side face image of the user are acquired, and then a front face feature and a side face feature of the user are acquired based on the front face image and the side face image of the user.

25 [0046] In step 23, a list of users with similar front face features is acquired based on

whether front face features of each group of users of multiple births are similar.

[0047] A list of users with similar front face features in the list of multiple births is determined by collecting front face features of the users in the list of multiple births for comparison. As shown in FIG. 2(b), the list with similar front face features in the figure is acquired based on
5 the list of multiple births, and thus is included in the range of the list of multiple births.

[0048] In step 24, a list with similar front face features and similar side face features is acquired for each group of users with similar front face features based on whether their side face features are similar.

[0049] For each group of users with similar front face features, a list with similar front face
10 features and similar side face features can be acquired by collecting side face features of the users for comparison and determining whether side face features of the users with similar front face features are also similar. As shown in FIG. 2(b), the list with similar front face features and similar side face features in the figure is acquired based on the list with similar front face features, and thus is included in the range of the list with similar front faces.

15 [0050] In step 120, a list of multiple births corresponding to the user is searched, based on the front face feature and the side face feature of the user, for a candidate user matching both the front face feature and the side face feature of the user.

[0051] The list of multiple births corresponding to the user is a list of multiple births with similar front face features and non-similar side face features, that is, the list of multiple births
20 corresponding to the shaded area shown in FIG. 2(b).

[0052] In step 130, it is determined, based on consistency between the candidate user and the user in the front face feature and the side face feature, whether the user succeeds in the authentication.

[0053] Optionally, the determining, based on consistency between the candidate user and
25 the user in the front face feature and the side face feature, whether the user succeeds in the

authentication includes the following two situations: 1. determining that the user succeeds in the authentication if the candidate user is consistent with the user in both the front face feature and the side face feature; and 2. determining that the user fails in the authentication if the candidate user is inconsistent with the user in the front face feature or the side face feature.

5 **[0054]** A front face feature and a side face feature of a user are acquired in response to a face authentication request of the user, then a list of multiple births corresponding to the user is searched, based on the front face feature and the side face feature of the user, for a candidate user matching both the front face feature and the side face feature of the user, wherein the list of multiple births corresponding to the user is a list of multiple births with similar front face features and non-
10 similar side face features, and finally, it can be determined, based on consistency between the candidate user and the user in the front face feature and the side face feature, whether the user succeeds in the authentication. As such, when the authenticated user is a user of multiple births, the front face feature and the side face feature of the user can be acquired and then compared with front face features and side face features of users in the pre-established list of multiple births to
15 determine whether the user succeeds in the authentication, thus solving the problem of identifying using face features of a user of multiple births in the prior art.

[0055] An authentication mode determination method is further provided in an embodiment of this specification. As shown in FIG. 3, it is a schematic diagram of an implementation process of an authentication mode determination method according to an
20 embodiment of this specification, including the following steps.

[0056] In step 310, user information of a user is acquired in response to a request for activating a face authentication mode from the user.

[0057] If a request for activating a face authentication mode is received from a user, user information of the user is acquired in response to the request for activating a face authentication
25 mode from the user. The user information of the user may specifically be an ID of the user, i.e., the

unique identification information of the user as described above.

[0058] In step 320, an authentication mode is determined for the user based on first user information with similar front face features and non-similar side face features in a list of multiple births, second user information with similar front face features and similar side face features in the
5 list of multiple births, and the user information of the user.

[0059] Optionally, the determining an authentication mode for the user based on first user information with similar front face features and non-similar side face features in a list of multiple births, second user information with similar front face features and similar side face features in the list of multiple births, and the user information of the user includes the following situations.

10 [0060] In Situation i, a front face feature and a side face feature of the user are acquired if the user information of the user is in the first user information; and an authentication mode is determined for the user based on the front face feature and the side face feature of the user. As the first user information is first user information with similar front face features and non-similar side face features in the list of multiple births, i.e., the user information corresponding to the shaded
15 area shown in FIG. 2(b), the front face feature and the side face feature of the user need to be collected as comparison features for performing face authentication on the user. When face authentication is performed on the user, a front face picture and a side face picture of the user need to be collected at the same time, and the front face feature and the side face feature corresponding to the front face picture and the side face picture collected when face authentication is performed
20 on the user are compared with the front face feature and the side face feature of the user collected when the user activates the face authentication mode, and it is determined based on a comparison result whether the user succeeds in the authentication.

[0061] In Situation ii, a front face feature of the user is acquired if the user information of the user is not in the first user information; and the authentication mode is determined for the user
25 based on the front face feature of the user. In this situation, if the user information of the user is

not in the first user information, it can be determined that the user information of the user is not in the second user information, either. In other words, the user does not belong to the users with similar front face features. Therefore, when the user activates the face authentication mode, it is possible that only a front face feature of the user is collected as a comparison feature for performing face authentication on the user. Then, when face authentication is performed on the user, it is only necessary to collect the front face picture of the user, compare a front face feature corresponding to the front face picture collected when face authentication is performed on the user with the front face feature collected when the user activates the authentication mode, and determine based on a comparison result whether the user succeeds in the authentication.

- 10 **[0062]** In Situation iii, the user is prompted to activate another authentication mode if the user information of the user is in the second user information, the another authentication mode being an authentication mode other than the face authentication mode. If the user information of the user is in the second user information, it indicates that the user is in the list of multiple births with similar front face features and similar side face features. In this situation, in order to improve the accuracy of the authentication result and ensure the security of the user information, the user can be prompted to activate another authentication mode, i.e., an authentication mode other than the face authentication, such as fingerprint recognition, password verification, and SMS verification code.

- 15 **[0063]** The authentication mode determination method provided in this specification is described in detail in the following with reference to the schematic diagram of a specific implementation process of determining an authentication mode shown in FIG. 4. As shown in FIG. 4, the method includes the following steps.

[0064] In step 41, a user ID is acquired in response to a request for activating a face authentication mode from the user.

- 25 **[0065]** In step 42, it is determined based on the user ID whether the user has activated the

face authentication mode, and if it is determined that the user has activated the face authentication mode, step 43 is performed.

[0066] In step 43, if it is determined that the user has activated the face authentication mode, the user is allowed to directly use the face authentication mode.

5 [0067] In step 44, if it is determined that the user has not activated the face authentication mode, it is prompted that the user is required to authorize activation of the face authentication mode.

[0068] In step 45, it is determined whether the user is in second user information, if it is determined that the user is in the second user information, step 46 is performed, and if it is
10 determined that the user is not in the second user information, step 47 is performed.

[0069] In step 46, if it is determined that the user is in the second user information, the user is prompted that activation of the face authentication mode fails.

[0070] In this case, in order to protect the security of user information and improve the accuracy of the authentication result, the user can be prompted to use another authentication mode,
15 that is, an authentication mode other than the face authentication mode.

[0071] In step 47, if it is determined that the user is not in the second user information, it is determined whether the user is in first user information.

[0072] In step 48, if it is determined that the user is in the first user information, a front face feature and a side face feature of the user are collected, and the authentication mode is
20 determined for the user based on the front face feature and the side face feature of the user.

[0073] That is, the front face feature and the side face feature of the user are collected as comparison features of the face authentication mode of the user. When face authentication is performed on the user, a front face picture and a side face picture of the user are collected, a front face feature and a side face feature corresponding to the front face picture and the side face picture
25 are extracted and compared with the front face feature and the side face feature collected when the

user activates the face authentication mode, if the comparison is successful, the user succeeds in the face authentication, and if the comparison is not successful, the user fails in the face authentication.

[0074] In step 49, a front face feature of the user is collected if the user information of the user is not in the first user information; and the authentication mode is determined for the user based on the front face feature of the user.

[0075] In this situation, it is possible to only collect the front face feature of the user. When face authentication is performed on such a user, it is possible to only collect a front face picture of the user, extract a front face feature corresponding to the front face picture and compare the front face feature with the front face feature collected when the user activates the face authentication mode. If the comparison is successful, the user succeeds in the face authentication, and if the comparison is not successful, the user fails in the face authentication.

[0076] In step 410, a list of users who have activated the face authentication mode is updated.

[0077] User information of a user is acquired in response to a request for activating a face authentication mode from the user, and then an authentication mode is determined for the user based on first user information with similar front face features in a list of multiple births, second user information with similar front face features and similar side face features in the list of multiple births, and the user information of the user. As such, when the user to activate the face authentication mode is a user of multiple births, a specific authentication mode can be determined for the user by determining whether the user is a user only with a similar front face feature in the list of multiple births, a user with both a similar front face feature and a similar side face feature in the list of multiple births, or a user with a non-similar front face feature in the list of multiple births, so that some users in the list of multiple births can also activate the face authentication mode.

[0078] FIG. 5 is a schematic structural diagram of an authentication apparatus 500

according to this specification. Referring to FIG. 5, in a software implementation manner, the authentication apparatus 500 can include an acquisition unit 501, a searching unit 502, and a determination unit 503.

[0079] The acquisition unit 501 is configured to acquire a front face feature and a side face
5 feature of a user in response to a face authentication request of the user.

[0080] The searching unit 502 is configured to search, based on the front face feature and
the side face feature of the user, a list of multiple births corresponding to the user for a candidate
user matching both the front face feature and the side face feature of the user, wherein the list of
multiple births corresponding to the user is a list of multiple births with similar front face features
10 and non-similar side face features.

[0081] The determination unit 503 is configured to determine, based on consistency
between the candidate user and the user in the front face feature and the side face feature, whether
the user succeeds in the authentication.

[0082] Optionally, in an implementation manner, the acquisition unit 501 is configured to:
15 determine whether the user is in a list of multiple births with similar front faces; and acquire the
front face feature and the side face feature of the user if the user is in the list of multiple births with
similar front face features.

[0083] Optionally, in an implementation manner, the determination unit 503 is configured
to: determine that the user succeeds in the authentication if the candidate user is consistent with
20 the user in both the front face feature and the side face feature; and determine that the user fails in
the authentication if the candidate user is inconsistent with the user in the front face feature or the
side face feature.

[0084] The authentication apparatus 500 can implement the method in the method
embodiment of FIG. 1 and FIGS. 2(a) and 2(b). Reference can be made to the authentication
25 method in the embodiments shown in FIG. 1 and FIGS. 2(a) and 2(b) for details, which will not be

elaborated here.

[0085] FIG. 6 is a schematic structural diagram of an authentication mode determination apparatus 600 according to this specification. Referring to FIG. 6, in a software implementation manner, the authentication mode determination apparatus 600 can include an acquisition unit 601
5 and a determination unit 602.

[0086] The acquisition unit 601 is configured to acquire user information of a user in response to a request for activating a face authentication mode from the user.

[0087] The determination unit 602 is configured to determine an authentication mode for the user based on first user information with similar front face features and non-similar side face
10 features in a list of multiple births, second user information with similar front face features and similar side face features in the list of multiple births, and the user information of the user.

[0088] Optionally, in an implementation manner, the determination unit 602 is configured to: acquire a front face feature and a side face feature of the user if the user information of the user is in the first user information; and determine the authentication mode for the user based on the
15 front face feature and the side face feature of the user.

[0089] Optionally, in an implementation manner, the determination unit 602 is configured to: acquire a front face feature of the user if the user information of the user is not in the first user information; and determine the authentication mode for the user based on the front face feature of the user.

20 [0090] Optionally, in an implementation manner, the determination unit 602 is configured to: prompt the user to activate another authentication mode if the user information of the user is in the second user information, the another authentication mode being an authentication mode other than the face authentication mode.

[0091] The authentication mode determination apparatus 600 can implement the method
25 in the method embodiment of FIG. 3 and FIG. 4. Reference can be made to the authentication mode

determination method in the embodiments shown in FIG. 3 and FIG. 4 for details, which will not be elaborated here.

[0092] FIG. 7 is a schematic structural diagram of an electronic device 700 according to an embodiment of this specification. Referring to FIG. 7, at the hardware level, the electronic device 700 includes a processor 702, and optionally further includes an internal bus 704, a network interface 706, and a memory. The memory may include an internal memory 708 such as a high-speed Random-Access Memory (RAM), or may further include a non-volatile memory 710 such as at least one magnetic disk memory. Definitely, the electronic device 700 may further include hardware required by other services.

10 [0093] The processor 702, the network interface 706, and the memory 708 and 710 may be interconnected through the internal bus 704, and the internal bus 704 may be an Industry Standard Architecture (ISA) bus, a Peripheral Component Interconnect (PCI) bus, an Extended Industry Standard Architecture (EISA) bus, or the like. The bus may be classified into an address bus, a data bus, a control bus, and the like. For ease of representation, only one double-sided arrow is shown in FIG. 7, but it does not mean that there is only one bus or one type of buses.

[0094] The memory is configured to store a program. Specifically, the program may include program codes including a computer operation instruction. The memory may include the internal memory and the non-volatile memory, and provides an instruction and data to the processor.

[0095] The processor reads, from the non-volatile memory, the corresponding computer program into the internal memory and runs the computer program, thus forming an authentication apparatus at the logic level. The processor executes the program stored in the memory, and is specifically configured to perform the following operations: acquiring a front face feature and a side face feature of a user in response to a face authentication request of the user; searching, based on the front face feature and the side face feature of the user, a list of multiple births corresponding to the user for a candidate user matching both the front face feature and the side face feature of the

25

user, wherein the list of multiple births corresponding to the user is a list of multiple births with similar front face features and non-similar side face features; and determining, based on consistency between the candidate user and the user in the front face feature and the side face feature, whether the user succeeds in the authentication.

5 [0096] The authentication method disclosed in the embodiments shown in FIG. 1 and FIGS. 2(a) and 2(b) of this specification can be applied to the processor or implemented by the processor. The processor may be an integrated circuit chip having a signal processing capability. In the process of implementation, various steps of the above method may be completed by an integrated logic circuit of hardware in the processor or an instruction in the form of software. The processor may
10 be a general-purpose processor, including a Central Processing Unit (CPU), a Network Processor (NP), etc.; or may be a Digital Signal Processor (DSP), an Application Specific Integrated Circuit (ASIC), a Field-Programmable Gate Array (FPGA) or another programmable logic device, discrete gate or transistor logic device, or discrete hardware component. The methods, steps, and logical block diagrams disclosed in the embodiments of this specification can be implemented or
15 performed. The general-purpose processor may be a microprocessor, or the processor may be any conventional processor or the like. The steps of the method disclosed in one or more embodiments of this specification may be directly performed by a hardware decoding processor, or may be performed by a combination of hardware and software modules in the decoding processor. The software module can be located in a mature storage medium in the field, such as a random-access
20 memory, a flash memory, a read-only memory, a programmable read-only memory or an electrically erasable programmable memory, and a register. The storage medium is located in the memory, and the processor reads the information in the memory and implements the steps of the above method in combination with its hardware.

 [0097] The electronic device can also perform the authentication method of FIG. 1 and
25 FIGS. 2(a) and 2(b), which will not be elaborated here in this specification.

[0098] Definitely, in addition to the software implementation manner, the electronic device in this specification does not exclude other implementation manners, such as logic devices or a combination of software and hardware, etc. In other words, the following processing procedure may not be performed only by various logic units, but also can be performed by hardware or logic devices.

[0099] FIG. 8 is a schematic structural diagram of an electronic device 800 according to an embodiment of this specification. Referring to FIG. 8, at the hardware level, the electronic device 800 includes a processor 802, and optionally further includes an internal bus 804, a network interface 806, and a memory. The memory may include an internal memory 808 such as a high-speed Random-Access Memory (RAM), or may further include a non-volatile memory 810 such as at least one magnetic disk memory. Definitely, the electronic device 800 may further include hardware required by other services.

[0100] The processor 802, the network interface 806, and the memory 808 and 810 may be interconnected through the internal bus 804, and the internal bus 804 may be an Industry Standard Architecture (ISA) bus, a Peripheral Component Interconnect (PCI) bus, an Extended Industry Standard Architecture (EISA) bus, or the like. The bus may be classified into an address bus, a data bus, a control bus, and the like. For ease of representation, only one double-sided arrow is shown in FIG. 8, but it does not mean that there is only one bus or one type of buses.

[0101] The memory is configured to store a program. Specifically, the program may include program codes including a computer operation instruction. The memory may include the internal memory and the non-volatile memory, and provides an instruction and data to the processor.

[0102] The processor reads, from the non-volatile memory, the corresponding computer program into the internal memory and runs the computer program, thus forming an authentication mode determination apparatus at the logic level. The processor executes the program stored in the memory, and is specifically configured to perform the following operations: acquiring user

information of a user in response to a request for activating a face authentication mode from the user; and determining an authentication mode for the user based on first user information with similar front face features and non-similar side face features in a list of multiple births, second user information with similar front face features and similar side face features in the list of multiple
5 births, and the user information of the user.

[0103] The authentication mode determination method disclosed in the embodiments shown in FIG. 3 and FIG. 4 of this specification can be applied to the processor or implemented by the processor. The processor may be an integrated circuit chip having a signal processing capability. In the process of implementation, various steps of the above method may be completed
10 by an integrated logic circuit of hardware in the processor or an instruction in the form of software. The processor may be a general-purpose processor, including a Central Processing Unit (CPU), a Network Processor (NP), etc.; or may be a Digital Signal Processor (DSP), an Application Specific Integrated Circuit (ASIC), a Field-Programmable Gate Array (FPGA) or another programmable logic device, discrete gate or transistor logic device, or discrete hardware component. The methods,
15 steps, and logical block diagrams disclosed in the embodiments of this specification can be implemented or performed. The general-purpose processor may be a microprocessor, or the processor may be any conventional processor or the like. The steps of the method disclosed in one or more embodiments of this application may be directly performed by a hardware decoding processor, or may be performed by a combination of hardware and software modules in the
20 decoding processor. The software module can be located in a mature storage medium in the field, such as a random-access memory, a flash memory, a read-only memory, a programmable read-only memory or an electrically erasable programmable memory, and a register. The storage medium is located in the memory, and the processor reads the information in the memory and implements the steps of the above method in combination with its hardware.

25 [0104] The electronic device can also perform the authentication mode determination

method in FIG. 3 and FIG. 4, which will not be elaborated here in this specification.

[0105] Definitely, in addition to the software implementation manner, the electronic device in this specification does not exclude other implementation manners, such as logic devices or a combination of software and hardware, etc. In other words, the following processing procedure
5 may not be performed only by various logic units, but also can be performed by hardware or logic devices.

[0106] In brief, the above description is merely example embodiments of this specification, and is not intended to limit the protection scope of this specification. Any modification, equivalent replacement, improvement and the like made within the spirit and principle of one or more
10 embodiments of this specification should be included in the protection scope of one or more embodiments of this specification.

[0107] The system, apparatus, module or unit illustrated in the above embodiments may be implemented by a computer chip or an entity, or by a product having a certain function. A typical implementation device is a computer. For example, the computer may be a personal computer, a
15 laptop computer, a cellular phone, a camera phone, a smart phone, a personal digital assistant, a media player, a navigation device, an email device, a game console, a tablet computer, a wearable device, or a combination of any of these devices.

[0108] The computer readable medium includes non-volatile and volatile media as well as movable and non-movable media, and may implement information storage by means of any
20 method or technology. The information may be a computer readable instruction, a data structure, and a module of a program or other data. Examples of the storage medium of a computer include, but are not limited to, a phase change memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), other types of RAMs, a ROM, an electrically erasable programmable read-only memory (EEPROM), a flash memory or other memory technologies, a
25 compact disk read-only memory (CD-ROM), a digital versatile disc (DVD) or other optical

storages, a cassette tape, a magnetic tape/magnetic disk storage or other magnetic storage devices, or any other non-transmission medium, and can be used to store information accessible to a computing device. The computer readable medium does not include transitory media, such as a modulated data signal and a carrier.

- 5 **[0109]** It should be further noted that the terms “include,” “comprise” or other variations thereof are intended to cover non-exclusive inclusion, so that a process, method, article or device including a series of elements not only includes the elements, but also includes other elements not expressly listed, or further includes elements inherent to the process, method, article or device. In the absence of more limitations, an element defined by "including a/an..." does not exclude that
- 10 the process, method, article or device including the element further has other identical elements.

- [0110]** Various embodiments in this specification are described progressively. The same or similar parts between the embodiments may be referenced to one another. In each embodiment, the focus of description is on the part that is different from other embodiment. Particularly, the system embodiment is described in a relatively simple manner because it is similar to the method
- 15 embodiment, and for related parts, reference can be made to the parts described in the method embodiment.