

METHOD AND APPARATUS FOR USER AUTHENTICATION BASED ON FEATURE INFORMATION

Technical Field

5 This specification relates to the field of identification technologies, and in particular, to a method and an apparatus for user authentication based on feature information.

Background

Face recognition, as a recognition technology with good user experience, is increasingly widely applied in many scenarios. The principle of the face recognition is
10 collecting a face image of a target user, extracting an image feature, comparing the image feature with a picture or image feature pre-stored by the target user in a system, and deciding the identity authenticity of the user according to a comparison result.

However, the existing face recognition technology cannot achieve a 100% accuracy rate. For example, a misrecognition may occur in such a special case as similar faces (e.g.,
15 identical twins, father and son, mother and daughter, "celebrity faces," and the like), and the misrecognition usually brings trouble to life or work of a user, or even causes an account and funds of the user to be stolen. Therefore, recognition of similar faces is a difficult problem in face recognition.

To prevent the aforementioned misrecognition, risky users who possibly have similar
20 faces are all shielded in the existing art, that is, risky users are not allowed to use face recognition. However, with the wide application of the face recognition technology, the user base of the face recognition technology also grows dramatically, which also causes a rapid increase in the number of users with similar looks. As a result, it is difficult to perform the shielding-based misrecognition prevention method in practical applications. In
25 addition, the shielding method cannot solve the misrecognition problem of similar faces

fundamentally.

Summary of the Invention

An objective of one or more embodiments of this specification is to provide a method and an apparatus for user authentication based on feature information, to improve an accuracy rate and a coverage rate of user authentication.

To solve the foregoing technical problem, one or more embodiments of this specification are implemented as follows:

In one aspect, one or more embodiments of this specification provide a method for user authentication based on feature information, including:

judging whether a user to be authenticated belongs to a similar user group, wherein the similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition; and

authenticating the user to be authenticated according to reference feature information in the similar user group if the user to be authenticated belongs to the similar user group.

Optionally, the authenticating the user to be authenticated according to reference feature information in the similar user group includes:

acquiring feature information collected for the user to be authenticated;

comparing the collected feature information with each piece of reference feature information in the similar user group to obtain a first comparison result; and

determining whether the user to be authenticated passes the authentication according to the first comparison result.

Optionally, the judging whether a user to be authenticated belongs to a similar user group includes:

acquiring identifier information of the user to be authenticated; and

judging whether the identifier information of the user to be authenticated matches identifier information of a similar user in a pre-stored similar user group; if yes, determining that the user to be authenticated belongs to the similar user group; otherwise, determining that the user to be authenticated does not belong to the similar user group.

5 Optionally, the preset similarity condition includes: a similarity degree of the reference feature information reaches a preset threshold.

Optionally, the preset distinguishability condition includes: based on comparisons of similarity degrees between the sample feature information of a similar user and each piece of reference feature information in the similar user group to which the similar user belongs,
10 a ratio of the number of successful similarity degree comparisons is greater than a preset ratio value.

Optionally, the comparing the collected feature information with each piece of reference feature information in the similar user group to obtain a first comparison result includes:

15 calculating a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information
20 as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated;

correspondingly, the determining whether the user to be authenticated passes the authentication according to the first comparison result includes:

determining that the user to be authenticated passes the authentication if the first
25 similarity degree is greater than the second similarity degree; and

determining that the user to be authenticated does not pass the authentication if the first similarity degree is not greater than the second similarity degree.

Optionally, the method further includes:

5 acquiring reference feature information and sample feature information corresponding to each one of at least two sample users, wherein the reference feature information of the at least two sample users meets the preset similarity condition;

calculating, for any of the sample users, similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user;

10 judging whether the at least two sample users meet the preset distinguishability condition according to the calculated similarity degrees; and

adding the at least two sample users to the same similar user group when the at least two sample users meet the preset distinguishability condition.

Optionally, the judging whether the at least two sample users meet the preset
15 distinguishability condition according to the calculated similarity degrees includes:

comparing a third similarity degree between the sample feature information corresponding to the sample user and the reference feature information corresponding to the sample user with a fourth similarity degree between the sample feature information corresponding to the sample user and the reference feature information corresponding to
20 the sample users other than the sample user, to obtain a second comparison result;

judging whether the third similarity degree is greater than the fourth similarity degree according to the second comparison result;

if yes, determining that a comparison of similarity degrees between the sample feature information corresponding to the sample user and the reference feature information
25 corresponding to each sample user is successful; otherwise, determining that the

comparison of similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user is failed; and

collecting statistics on a ratio of the number of successful similarity degree
5 comparisons, and determining that the at least two sample users meet the preset distinguishability condition when the ratio of the number is greater than the preset ratio value.

Optionally, the method further includes:

acquiring a global user information database when the user to be authenticated does not
10 belong to the similar user group, the global user information database including reference feature information and identifier information corresponding to each one of users in excess of a preset number;

determining reference feature information corresponding to the user to be authenticated in the global user information database according to identifier information corresponding
15 to the user to be authenticated; and

authenticating the user to be authenticated according to the reference feature information corresponding to the user to be authenticated.

Optionally, the feature information includes at least one piece of the following information: a face feature, an iris feature, a fingerprint, and an eyeprint, and the identifier
20 information includes at least one of an ID number, a communication number, a name, and predetermined identifier information.

In another aspect, one or more embodiments of this specification provide a method for user authentication based on feature information, including:

receiving an authentication request of a user to be authenticated, the authentication
25 request including identifier information of the user to be authenticated;

judging whether the user to be authenticated belongs to a similar user group according to the identifier information of the user to be authenticated, wherein the similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition;

5 if the user to be authenticated belongs to the similar user group, acquiring feature information collected for the user to be authenticated, calculating a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and reference feature information corresponding
10 to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

 determining that the user to be authenticated passes the authentication if the first
15 similarity degree is greater than the second similarity degree.

In another aspect, one or more embodiments of this specification provide an apparatus for user authentication based on feature information, including:

 a first judgment module configured to judge whether a user to be authenticated belongs to a similar user group, wherein the similar user group includes at least two similar users,
20 and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition; and

 a first authentication module configured to authenticate the user to be authenticated according to reference feature information in the similar user group if the user to be authenticated belongs to the similar user group.

25 Optionally, the first authentication module includes:

a first acquisition unit configured to acquire feature information collected for the user to be authenticated;

a comparison unit configured to compare the collected feature information with each piece of reference feature information in the similar user group to obtain a first comparison
5 result; and

a determining unit configured to determine whether the user to be authenticated passes the authentication according to the first comparison result.

Optionally, the first judgment module includes:

an identifier information acquisition unit configured to acquire identifier information of
10 the user to be authenticated; and

a first judgment unit configured to judge whether the identifier information of the user to be authenticated matches identifier information of a similar user in a pre-stored similar user group; if yes, determine that the user to be authenticated belongs to the similar user group; otherwise, determine that the user to be authenticated does not belong to the similar
15 user group.

Optionally, the preset similarity condition includes: a similarity degree of the reference feature information reaches a preset threshold.

Optionally, the preset distinguishability condition includes: based on comparisons of similarity degrees between the sample feature information of a similar user and each piece
20 of reference feature information in the similar user group to which the similar user belongs, a ratio of the number of successful similarity degree comparisons is greater than a preset ratio value.

Optionally, the comparison unit is configured to calculate a first similarity degree between the collected feature information and reference feature information corresponding
25 to a first similar user in the similar user group, and calculate a second similarity degree

between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

correspondingly, the determining unit is configured to determine that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree; and determine that the user to be authenticated does not pass the authentication if the first similarity degree is not greater than the second similarity degree.

Optionally, the apparatus further includes a creation module configured to create the similar user group;

wherein the creation module includes:

a second acquisition unit configured to acquire reference feature information and sample feature information corresponding to each one of at least two sample users, wherein the reference feature information of the at least two sample users meets the preset similarity condition;

a calculation unit configured to calculate, for any of the sample users, similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user;

a second judgment unit configured to judge whether the at least two sample users meet the preset distinguishability condition according to the calculated similarity degrees; and

an adding unit configured to add the at least two sample users to the same similar user group when the at least two sample users meet the preset distinguishability condition.

Optionally, the judgment unit is configured to compare a third similarity degree between the sample feature information corresponding to the sample user and the reference

feature information corresponding to the sample user with a fourth similarity degree between the sample feature information corresponding to the sample user and the reference feature information corresponding to the sample users other than the sample user, to obtain a second comparison result; judge whether the third similarity degree is greater than the fourth similarity degree according to the second comparison result; if yes, determine that a comparison of similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user is successful; otherwise, determine that the comparison of similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user is failed; and collect statistics on a ratio of the number of successful similarity degree comparisons, and determine that the at least two sample users meet the preset distinguishability condition when the ratio of the number is greater than the preset ratio value.

Optionally, the apparatus further includes:

an acquisition module configured to acquire a global user information database when the user to be authenticated does not belong to the similar user group, the global user information database including reference feature information and identifier information corresponding to each one of users in excess of a preset number;

a determining module configured to determine reference feature information corresponding to the user to be authenticated in the global user information database according to identifier information corresponding to the user to be authenticated; and

a second authentication module configured to authenticate the user to be authenticated according to the reference feature information corresponding to the user to be authenticated.

Optionally, the feature information includes at least one piece of the following information: a face feature, an iris feature, a fingerprint, and an eyeprint, and the identifier

information includes at least one of an ID number, a communication number, a name, and predetermined identifier information.

In another aspect, one or more embodiments of this specification provide an apparatus for user authentication based on feature information, including:

5 a receiving module configured to receive an authentication request of a user to be authenticated, the authentication request including identifier information of the user to be authenticated;

a second judgment module configured to judge whether the user to be authenticated belongs to a similar user group according to the identifier information of the user to be
10 authenticated, wherein the similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition;

a calculation module configured to, if the user to be authenticated belongs to the similar user group, acquire feature information collected for the user to be authenticated, calculate
15 a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculate a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information as that of the user
20 to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

a determining module configured to determine that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree.

In further another aspect, one or more embodiments of this specification provide an
25 apparatus for user authentication based on feature information, including:

a processor; and

a memory configured to store computer executable instructions, wherein the processor is enabled to perform the following steps when the computer executable instructions are executed:

5 judging whether a user to be authenticated belongs to a similar user group, wherein the similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition; and

 authenticating the user to be authenticated according to reference feature information in
10 the similar user group if the user to be authenticated belongs to the similar user group.

In further another aspect, one or more embodiments of this specification provide an apparatus for user authentication based on feature information, including:

a processor; and

 a memory configured to store computer executable instructions, wherein the processor
15 is enabled to perform the following steps when the computer executable instructions are executed:

 receiving an authentication request of a user to be authenticated, the authentication request including identifier information of the user to be authenticated;

 judging whether the user to be authenticated belongs to a similar user group according
20 to the identifier information of the user to be authenticated, wherein the similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition;

 if the user to be authenticated belongs to the similar user group, acquiring feature information collected for the user to be authenticated, calculating a first similarity degree
25 between the collected feature information and reference feature information corresponding

to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information as that of the user to be authenticated, and the
5 second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

determining that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree.

In further another aspect, one or more embodiments of this specification provide a
10 storage medium for storing computer executable instructions, wherein the following processes are implemented when the computer executable instructions are executed:

judging whether a user to be authenticated belongs to a similar user group, wherein the similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset
15 distinguishability condition; and

authenticating the user to be authenticated according to reference feature information in the similar user group if the user to be authenticated belongs to the similar user group.

In further another aspect, one or more embodiments of this specification provide a
20 storage medium for storing computer executable instructions, wherein the following processes are implemented when the computer executable instructions are executed:

receiving an authentication request of a user to be authenticated, the authentication request including identifier information of the user to be authenticated;

judging whether the user to be authenticated belongs to a similar user group according to the identifier information of the user to be authenticated, wherein the similar user group
25 includes at least two similar users, and the similar users are users whose reference feature

information meets a preset similarity condition and a preset distinguishability condition;

if the user to be authenticated belongs to the similar user group, acquiring feature information collected for the user to be authenticated, calculating a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

determining that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree.

By using the technical solution of one or more embodiments of this specification, it is first judged whether a user to be authenticated belongs to a similar user group, and if the user to be authenticated belongs to the similar user group, the user to be authenticated is authenticated according to reference feature information in the similar user group, wherein the similar user group includes at least two similar users, and the at least two similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition. It can be known that this technical solution can implement authentication for the user to be authenticated by using the similar user group to which similar users meeting the preset similarity condition and the preset distinguishability condition belong. Therefore, the user to be authenticated can be distinguished from a similar user thereof, thus preventing misrecognition between multiple similar users (for example, faces of father and son, identical twins, and so on), and further improving an accuracy rate of the user authentication. In addition, compared with the existing art in

which authentication for similar users is shielded, this technical solution greatly improves a coverage rate of the user authentication.

Brief Description of the Drawings

In order to illustrate the technical solutions in one or more embodiments of this specification or the prior art more clearly, the accompanying drawings required for describing the one or more embodiment or the prior art are introduced briefly in the following. It is apparent that the accompanying drawings in the following description are only some embodiments recorded in one or more embodiments of this specification. Those of ordinary skill in the art can obtain other drawings according to the accompanying drawings without creative efforts.

FIG. 1 is a schematic flowchart of a method for user authentication based on feature information according to an embodiment of this specification;

FIG. 2 is a schematic flowchart of a method for creating a similar user group according to an embodiment of this specification;

FIG. 3 is a schematic diagram of a manner of creating a similar user group according to Embodiment 1 of this specification;

FIG. 4 is a schematic diagram of a manner of creating a similar user group according to Embodiment 2 of this specification;

FIG. 5 is a schematic diagram of another manner of creating a similar user group according to Embodiment 2 of this specification;

FIG. 6 is a schematic flowchart of a method for user authentication based on feature information according to another embodiment of this specification;

FIG. 7 is a schematic block diagram of an apparatus for user authentication based on feature information according to an embodiment of this specification;

FIG. 8 is a schematic block diagram of an apparatus for user authentication based on

feature information according to another embodiment of this specification; and

FIG. 9 is a schematic block diagram of an apparatus for user authentication based on feature information according to another embodiment of this specification.

Detailed Description

5 One or more embodiments of this specification provide a method and an apparatus for user authentication based on feature information, to improve an accuracy rate and a coverage rate of user authentication.

 In order to help those skilled in the art better understand the technical solutions in one or more embodiments of this specification, the technical solutions in one or more
10 embodiments of this specification are described clearly and completely in the following with reference to the accompanying drawings in one or more embodiments of this specification. Apparently, the described embodiments are merely some, rather than all, of the embodiments of this specification. Based on one or more embodiments of this specification, all other embodiments obtained by those of ordinary skill in the art without
15 creative efforts should belong to the protection scope of the one or more embodiments of this specification.

 FIG. 1 is a schematic flowchart of a method for user authentication based on feature information according to an embodiment of this specification. As shown in FIG. 1, the method includes the following steps:

20 In step S102, it is judged whether a user to be authenticated belongs to a similar user group.

 The similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition. When similar users are stored in the similar user group,
25 identifier information of each similar user is stored corresponding to the similar user. As

such, during the specific implementation, identifier information of the user to be authenticated can be matched with the identifier information of each similar user in the similar user group. If there is a similar user matching the identifier information of the user to be authenticated, the user to be authenticated belongs to the similar user group where the similar user is located; and if there is no similar user matching the identifier information of the user to be authenticated, the user to be authenticated does not belong to the similar user group.

In step S104, the user to be authenticated is authenticated according to reference feature information in the similar user group if the user to be authenticated belongs to the similar user group.

In this embodiment, whether the user to be authenticated belongs to the similar user group may be judged according to the identifier information or feature information of the user to be authenticated.

When the judgment is made according to the identifier information of the user to be authenticated, step S102 may include the following steps: first, acquiring the identifier information of the user to be authenticated; then judging whether the identifier information of the user to be authenticated matches identifier information of a similar user in a pre-stored similar user group; if yes, determining that the user to be authenticated belongs to the similar user group; otherwise, determining that the user to be authenticated does not belong to the similar user group. In the pre-stored similar user group, each similar user is associated with corresponding identifier information. Therefore, whether the user to be authenticated belongs to the similar user group can be judged through matching of the identifier information. The identifier information includes at least one of an ID number, a communication number, a name, and predetermined identifier information. The predetermined identifier information may be information pre-stored on a server side by the

user to be authenticated and used for identifying the identity of the user, e.g., a specified numeric string, or a specified text.

When the judgment is made according to the feature information of the user to be authenticated, each similar user in the pre-stored similar user group is associated with
5 corresponding reference feature information, and the judgment can be made by comparing the feature information of the user to be authenticated with the reference feature information of the similar users in the pre-stored similar user group. Therefore, step S102 may include the following steps: first, acquiring the feature information of the user to be authenticated; then judging whether the feature information of the user to be authenticated
10 matches reference feature information of a similar user in the pre-stored similar user group; if yes, determining that the user to be authenticated belongs to the similar user group; otherwise, determining that the user to be authenticated does not belong to the similar user group.

The authentication includes security authentication. The reference feature information
15 in the similar user group refers to feature information with a unique identification function which is pre-stored on the server side by each similar user in the similar user group, wherein the feature information may include at least one piece of the following information: a face feature, an iris feature, a fingerprint, and an eyeprint.

In this embodiment, the reference feature information includes feature information with
20 a unique identification function which is pre-stored on the server side by users, and is mainly used to be compared with other feature information in the authentication process. The selection of the reference feature information is not limited in this embodiment. The reference feature information may be standard feature information that can meet established criteria, non-standard feature information, preferred feature information
25 selected from multiple pieces of feature information according to a given condition, or the

like.

By using the technical solution of one or more embodiments of this specification, it is first judged whether a user to be authenticated belongs to a similar user group, and if the user to be authenticated belongs to the similar user group, the user to be authenticated is authenticated according to reference feature information in the similar user group, wherein the similar user group includes at least two similar users, and the at least two similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition. It can be known that this technical solution can implement authentication for the user to be authenticated by using the similar user group to which similar users meeting the preset similarity condition and the preset distinguishability condition belong. Therefore, the user to be authenticated can be distinguished from a similar user thereof, thus preventing misrecognition between multiple similar users (for example, faces of father and son, identical twins, and so on), and further improving an accuracy rate of the user authentication. In addition, compared with the existing art in which authentication for similar users is shielded, this technical solution greatly improves a coverage rate of the user authentication.

A similar user group needs to be established in advance before the foregoing steps S102 to S104 are performed. FIG. 2 is a schematic flowchart of a method for creating a similar user group according to an embodiment of this specification. As shown in FIG. 2, the method for creating a similar user group may include the following steps S202 to S210:

In step S202, reference feature information and sample feature information corresponding to each one of at least two sample users are acquired.

During selection of sample users, obviously dissimilar users can be avoided, and users with a higher similarity degree should be selected as sample users as much as possible, so as to improve the efficiency of creating the similar user group. For example, father and son,

sisters, twins, or the like with similar looks are selected as sample users. Preferably, the reference feature information of the at least two sample users meets a preset similarity condition, and the preset similarity condition includes that a similarity degree of the reference feature information reaches a preset threshold.

5 Reference feature information corresponding to a sample user refers to feature information with a unique identification function which is pre-stored on a server side by the user. Sample feature information corresponding to a sample user may include one or more pieces of feature information of the sample user which passes historical authentication. The feature information may include at least one piece of the following
10 information: a face feature, an iris feature, a fingerprint, and an eyeprint.

 In step S204, for any sample user, similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user are calculated.

 In this step, during the similarity degree comparison of the feature information, a
15 feature vector of each piece of feature information may be determined, and then a feature vector distance between different feature information is calculated to determine a similarity degree between the different feature information. If the feature information is face images, a similarity degree between different face images can also be determined by determining an eigenface (that is, a set of feature vectors for the face recognition problem in the
20 computer vision field) corresponding to each face image, etc. The aforementioned similarity degree comparison methods for feature information belong to the existing art, and detailed description thereof will not be repeated here.

 In step S206, it is determined whether the at least two sample users meet a preset distinguishability condition according to the calculated similarity degrees; if yes, step S208
25 is performed; otherwise, step S210 is performed.

The preset distinguishability condition may include: based on comparisons of similarity degrees between the sample feature information of any sample user and the reference feature information corresponding to each sample user, a ratio of the number of successful similarity degree comparisons is greater than a preset ratio value. Based on the preset distinguishability condition, whether the at least two sample users meet the preset distinguishability condition may be judged through the following implementation during execution of step S206:

First, a third similarity degree between the sample feature information corresponding to the sample user and the reference feature information corresponding to the sample user is compared with a fourth similarity degree between the sample feature information corresponding to the sample user and the reference feature information corresponding to the sample users other than the sample user, to obtain a comparison result. Then, it is judged whether the third similarity degree is greater than the fourth similarity degree according to the comparison result; if yes, it is determined that a comparison of similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user is successful; otherwise, it is determined that the comparison of similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user is failed. Finally, statistics is collected on a ratio of the number of successful similarity degree comparisons, and it is determined that the at least two sample users meet the preset distinguishability condition when the ratio of the number is greater than the preset ratio value.

Definitely, in addition to the ratio of the number of successful similarity degree comparisons as in this embodiment, statistics may also be made on the number of successful similarity degree comparisons, and when the number of successful similarity

degree comparisons reaches a preset number, it can be determined that the at least two sample users meet the preset distinguishability condition. Alternatively, statistics may also be made on the number of failed similarity degree comparisons, and when the number of failed similarity degree comparisons reaches another preset number, it can be determined
5 that the at least two sample users do not meet the preset distinguishability condition.

It should be noted that, in the foregoing implementation, "third" and "fourth" in the third similarity degree and the fourth similarity degree are merely used for distinguishing similarity degrees between different feature information, and do not have other meanings.

In step S208, the at least two sample users are added to the same similar user group.

10 In step S210, it is determined that the at least two sample users cannot be added to the same similar user group.

How to create a similar user group according to the method in this embodiment is described below with two embodiments. In the following two embodiments, it can be determined that the at least two sample users meet the preset distinguishability condition
15 only when the ratio of the number of successful similarity degree comparisons is 100% (that is, similarity degree comparisons between all pieces of the sample feature information and the reference feature information corresponding to each sample user are all successful).

Embodiment 1

In this embodiment, the feature information is a face feature; thus, the reference feature
20 information is a reference face feature, and the sample feature information is a sample face feature.

First, step S202 is performed by selecting two sample users A and B. Each sample user corresponds to one reference face feature and one sample face feature. It is assumed that the sample user A corresponds to a reference face feature A1 and a sample face feature A2,
25 and the sample user B corresponds to a reference face feature B1 and a sample face feature

B2.

Then, step S204 is performed. For the sample user A, similarity degrees between the sample face feature A2 and the reference face feature A1 and between the sample face feature A2 and the reference face feature B1 are calculated respectively; for the sample user B, similarity degrees between the sample face feature B2 and the reference face feature A1 and between the sample face feature B2 and the reference face feature B1 are calculated respectively.

Next, step S206 is performed. For the sample user A, it is compared whether the similarity degree between the sample face feature A2 and the reference face feature A1 is greater than the similarity degree between the sample face feature A2 and the reference face feature B1, and if yes, it is determined that the comparison of similarity degrees between the sample face feature A2 and each reference face feature is successful; and for the sample user B, it is compared whether the similarity degree between the sample face feature B2 and the reference face feature B1 is greater than the similarity degree between the sample face feature B2 and the reference face feature A1, and if yes, it is determined that the comparison of similarity degrees between the sample face feature B2 and each reference face feature is successful.

FIG. 3 is a schematic diagram of a manner of creating a similar user group according to Embodiment 1 of this specification. As shown in FIG. 3, "successful" displayed under the sample face feature A2 represents that the comparison of similarity degrees between the sample face feature A2 and each reference face feature is successful, and "successful" displayed under the sample face feature B2 represents that the comparison of similarity degrees between the sample face feature B2 and each reference face feature is successful. The sample user A and the sample user B can be added to the same similar user group only when the comparison of similarity degrees between the sample face feature A2

corresponding to the sample user A and each reference face feature is successful and the comparison of similarity degrees between the sample face feature B2 corresponding to the sample user B and each reference face feature is successful; otherwise, the sample user A and the sample user B cannot be added to the similar user group if any similarity degree comparison is failed.

Embodiment 2

In this embodiment, the feature information is a face feature; thus, the reference feature information is a reference face feature, and the sample feature information is a sample face feature.

First, step S202 is performed by selecting two sample users A and B. Each sample user corresponds to one reference face feature and three sample face features. It is assumed that the sample user A corresponds to a reference face feature A1 as well as a sample face feature A2, a sample face feature A3, and a sample face feature A4; the sample user B corresponds to a reference face feature B1 as well as a sample face feature B2, a sample face feature B3, and a sample face feature B4.

Then, step S204 is performed. For the sample user A, similarity degrees between the sample face feature A2 and the reference face feature A1 and between the sample face feature A2 and the reference face feature B1 are calculated respectively; similarity degrees between the sample face feature A3 and the reference face feature A1 and between the sample face feature A3 and the reference face feature B1 are calculated respectively; and similarity degrees between the sample face feature A4 and the reference face feature A1 and between the sample face feature A4 and the reference face feature B1 are calculated respectively.

For the sample user B, similarity degrees between the sample face feature B2 and the reference face feature A1 and between the sample face feature B2 and the reference face

feature B1 are calculated respectively; similarity degrees between the sample face feature B3 and the reference face feature A1 and between the sample face feature B3 and the reference face feature B1 are calculated respectively; and similarity degrees between the sample face feature B4 and the reference face feature A1 and between the sample face feature B4 and the reference face feature B1 are calculated respectively.

Next, step S206 is performed. For the sample user A, it is compared whether the similarity degree between the sample face feature A2 and the reference face feature A1 is greater than the similarity degree between the sample face feature A2 and the reference face feature B1; if yes, it is determined that the comparison of similarity degrees between the sample face feature A2 and each reference face feature is successful; otherwise, it is determined that the comparison of similarity degrees between the sample face feature A2 and each reference face feature is failed. Moreover, it is compared whether the similarity degree between the sample face feature A3 and the reference face feature A1 is greater than the similarity degree between the sample face feature A3 and the reference face feature B1; if yes, it is determined that the comparison of similarity degrees between the sample face feature A3 and each reference face feature is successful; otherwise, it is determined that the comparison of similarity degrees between the sample face feature A3 and each reference face feature is failed. Moreover, it is compared whether the similarity degree between the sample face feature A4 and the reference face feature A1 is greater than the similarity degree between the sample face feature A4 and the reference face feature B1; if yes, it is determined that the comparison of similarity degrees between the sample face feature A4 and each reference face feature is successful; otherwise, it is determined that the comparison of similarity degrees between the sample face feature A4 and each reference face feature is failed.

For the sample user B, it is compared whether the similarity degree between the sample

face feature B2 and the reference face feature B1 is greater than the similarity degree between the sample face feature B2 and the reference face feature A1; if yes, it is determined that the comparison of similarity degrees between the sample face feature B2 and each reference face feature is successful; otherwise, it is determined that the comparison of similarity degrees between the sample face feature B2 and each reference face feature is failed. Moreover, it is compared whether the similarity degree between the sample face feature B3 and the reference face feature B1 is greater than the similarity degree between the sample face feature B2 and the reference face feature A1; if yes, it is determined that the comparison of similarity degrees between the sample face feature B3 and each reference face feature is successful; otherwise, it is determined that the comparison of similarity degrees between the sample face feature B3 and each reference face feature is failed. Moreover, it is compared whether the similarity degree between the sample face feature B4 and the reference face feature B1 is greater than the similarity degree between the sample face feature B4 and the reference face feature A1; if yes, it is determined that the comparison of similarity degrees between the sample face feature B4 and each reference face feature is successful; otherwise, it is determined that the comparison of similarity degrees between the sample face feature B4 and each reference face feature is failed.

FIG. 4 and FIG. 5 are schematic diagrams of manners of creating a similar user group according to Embodiment 2 of this specification. As shown in FIG. 4 and FIG. 5, "successful" or "failed" on the right side of each sample face feature is used to represent a result of the comparison of similarity degrees between the corresponding sample face feature and each reference face feature. In FIG. 4, the comparisons of similarity degrees between the sample face features A2, A3, A4 and each reference face feature are all successful, and the comparisons of similarity degrees between sample face features B2, B3,

B4 and each reference face feature are all successful as well. Therefore, it can be determined that the sample user A and the sample user B can be added to the same similar user group. In FIG. 5, because the comparison of similarity degrees between the sample face feature A4 and each reference face feature is failed, the sample user A and the sample user B cannot be added to the same similar user group.

After the similar user group is created according to the above method, user authentication can be performed according to the method described in steps S102 to S104. The steps S102 to S104 are described in detail below.

First, before step S102 is performed, an authentication request of the user to be authenticated is received. The authentication request may include identifier information of the user to be authenticated. The identifier information includes at least one of an ID number, a communication number, a name, and predetermined identifier information. The predetermined identifier information may be information pre-stored on a server side by the user to be authenticated and used for identifying the identity of the user, e.g., a specified numeric string, or a specified text.

After the authentication request is received, step S102 is continued to be performed. It is judged whether the user to be authenticated belongs to the similar user group according to the identifier information of the user to be authenticated. The similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition

In an embodiment, the preset similarity condition may include: a similarity degree of the reference feature information reaches a preset threshold. The preset distinguishability condition may include: based on comparisons of similarity degrees between the sample feature information of a similar user and each piece of reference feature information in the similar user group to which the similar user belongs, a ratio of the number of successful

similarity degree comparisons is greater than a preset ratio value. Detailed description has been given for the similar user group in the above embodiments, which will not be repeated in detail here.

After it is judged whether the user to be authenticated belongs to the similar user group, 5 step S104 is continued to be performed, that is, if the user to be authenticated belongs to the similar user group, the user to be authenticated is authenticated according to reference feature information in the similar user group. Specific authentication may include the following steps:

In step 1, feature information collected for the user to be authenticated is acquired. A 10 collection time of the feature information of the user to be authenticated is not limited in this embodiment. For example, the feature information of the user to be authenticated may be collected after the authentication request of the user to be authenticated is received, or the feature information of the user to be authenticated may be collected after it is judged whether the user to be authenticated belongs to the similar user group, or the feature 15 information of the user to be authenticated may be collected before the user to be authenticated is authenticated according to the reference feature information in the similar user group when it is judged that the user to be authenticated belongs to the similar user group.

In step 2, the collected feature information is compared with each piece of reference 20 feature information in the similar user group to obtain a comparison result.

In an embodiment, step 2 may be implemented in the following manner: first, calculating a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and 25 reference feature information corresponding to a second similar user in the similar user

group, wherein the first similar user is a similar user whose identifier information is the same as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; then, judging whether the first similarity degree is greater than the second similarity degree; if
5 yes, determining that the collected feature information matches the reference feature information corresponding to the first similar user; otherwise, determining that the collected feature information matches the reference feature information corresponding to the second similar user.

In step 3, it is determined whether the user to be authenticated passes the authentication
10 according to the comparison result. Specifically, when the comparison result is that the collected feature information matches the reference feature information corresponding to the first similar user, that is, the first similarity degree is greater than the second similarity degree, it is determined that the user to be authenticated passes the authentication; when
15 the first comparison result is that the collected feature information matches the reference feature information corresponding to the second similar user, that is, the first similarity degree is not greater than the second similarity degree, it is determined that the user to be authenticated does not pass the authentication.

The case where the feature information is a face feature and security authentication is carried out for the user to be authenticated is taken as an example. It is assumed that a
20 collected face feature of the user to be authenticated is A, identifier information is "XXX0", and the user to be authenticated belongs to a similar user group including similar users M and N. In the similar user group, the similar user M corresponds to identifier information "XXX0" and a reference face feature B1; the similar user N corresponds to identifier information "XXX1" and a reference face feature B2. In this case, during authentication for
25 the user to be authenticated, a first similarity degree between the face feature A and the

reference face feature B1 corresponding to a first similar user (that is, the similar user M whose identifier information is the same as that of the user to be authenticated) in the similar user group, and a first similarity degree between the face feature A and the reference face feature B2 corresponding to a second similar user (that is, the similar user N
5 whose identifier information is different from that of the user to be authenticated) in the similar user group are calculated first. Secondly, it is judged whether the first similarity degree is greater than the second similarity degree. It is assumed that the first similarity degree is 98%, and the second similarity degree is 90%. Because the first similarity degree is greater than the second similarity degree, it can be determined that the face feature A of
10 the user to be authenticated matches the reference face feature B1 corresponding to the similar user M. In this case, the user to be authenticated passes the security authentication. It is assumed that the first similarity degree is 90%, and the second similarity degree is 98%. Because the second similarity degree is greater than the first similarity degree, it can be determined that the face feature A of the user to be authenticated matches the
15 reference face feature B2 corresponding to the similar user N. In this case, the user to be authenticated does not pass the security authentication.

In an embodiment, the foregoing method can further be implemented as steps S602 to S612 shown in FIG. 6:

In step S602, an authentication request of a user to be authenticated is received, the
20 authentication request including identifier information of the user to be authenticated.

In step S604, it is judged whether the user to be authenticated belongs to a similar user group according to the identifier information of the user to be authenticated; if yes, step S606 is performed; otherwise, step S608 is performed.

In step S606, the user to be authenticated is authenticated according to reference
25 feature information in the similar user group.

In step S608, a global user information database is acquired, the global user information database including reference feature information and identifier information corresponding to each one of users in excess of a preset number.

5 In step S610, reference feature information corresponding to the user to be authenticated is determined in the global user information database according to the identifier information corresponding to the user to be authenticated.

In step S612, the user to be authenticated is authenticated according to the reference feature information corresponding to the user to be authenticated.

In this embodiment, if the user to be authenticated belongs to the similar user group,
10 the user to be authenticated is authenticated according to the reference feature information in the similar user group; and if the user to be authenticated does not belong to the similar user group, the user to be authenticated is authenticated according to the reference feature information in the global user information database. It can be seen that the technical solution not only can authenticate ordinary users, but also can accurately authenticate
15 similar users who cannot be recognized easily, thus preventing misrecognition between multiple similar users (for example, faces of father and son, identical twins, and so on), and further improving an accuracy rate and a coverage rate of the user authentication.

In conclusion, specific embodiments of this subject have been described. Other embodiments fall within the scope of the appended claims. In some cases, actions recorded
20 in the claims can be performed in different sequences and can still achieve the expected result. In addition, the processes depicted in the drawings do not necessarily require the shown particular sequence or a continuous sequence to achieve the expected result. In some implementations, multi-task processing and concurrent processing may be beneficial.

Described above is a method for generating a data relationship model according to one
25 or more embodiments of this specification. Based on the same conception, one or more

embodiments of this specification further provide an apparatus for user authentication based on feature information.

FIG. 7 is a schematic block diagram of an apparatus for user authentication based on feature information according to an embodiment of this specification. As shown in FIG. 7,
5 the apparatus includes:

a first judgment module 710 configured to judge whether a user to be authenticated belongs to a similar user group, wherein the similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition; and

10 a first authentication module 720 configured to authenticate the user to be authenticated according to reference feature information in the similar user group if the user to be authenticated belongs to the similar user group.

Optionally, the first authentication module 720 includes:

a first acquisition unit configured to acquire feature information collected for the user
15 to be authenticated;

a comparison unit configured to compare the collected feature information with each piece of reference feature information in the similar user group to obtain a first comparison result; and

a determining unit configured to determine whether the user to be authenticated passes
20 the authentication according to the first comparison result.

Optionally, the first judgment module 710 includes:

an identifier information acquisition unit configured to acquire identifier information of the user to be authenticated; and

a first judgment unit configured to judge whether the identifier information of the user
25 to be authenticated matches identifier information of a similar user in a pre-stored similar

user group; if yes, determine that the user to be authenticated belongs to the similar user group; otherwise, determine that the user to be authenticated does not belong to the similar user group.

Optionally, the preset similarity condition includes: a similarity degree of the reference
5 feature information reaches a preset threshold.

Optionally, the preset distinguishability condition includes: based on comparisons of similarity degrees between the sample feature information of a similar user and each piece of reference feature information in the similar user group to which the similar user belongs, a ratio of the number of successful similarity degree comparisons is greater than a preset
10 ratio value.

Optionally, the comparison unit is configured to calculate a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculate a second similarity degree between the collected feature information and reference feature information corresponding
15 to a second similar user in the similar user group, wherein the first similar user is a similar user whose identifier information is the same as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

correspondingly, the determining unit is configured to determine that the user to be
20 authenticated passes the authentication if the first similarity degree is greater than the second similarity degree; and determine that the user to be authenticated does not pass the authentication if the first similarity degree is not greater than the second similarity degree.

Optionally, the comparison unit is configured to determine that the user to be authenticated passes the authentication when the first comparison result is that the
25 collected feature information matches the reference feature information corresponding to

the first similar user; and determine that the user to be authenticated does not pass the authentication when the first comparison result is that the collected feature information matches the reference feature information corresponding to the second similar user.

Optionally, the apparatus further includes a creation module configured to create the
5 similar user group;

wherein the creation module includes:

a second acquisition unit configured to acquire reference feature information and sample feature information corresponding to each one of at least two sample users, wherein the reference feature information of the at least two sample users meets the preset
10 similarity condition;

a calculation unit configured to calculate, for any of the sample users, similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user;

a second judgment unit configured to judge whether the at least two sample users meet
15 the preset distinguishability condition according to the calculated similarity degrees; and

an adding unit configured to add the at least two sample users to the same similar user group when the at least two sample users meet the preset distinguishability condition.

Optionally, the judgment unit is configured to compare a third similarity degree between the sample feature information corresponding to the sample user and the reference
20 feature information corresponding to the sample user with a fourth similarity degree between the sample feature information corresponding to the sample user and the reference feature information corresponding to the sample users other than the sample user, to obtain a second comparison result; judge whether the third similarity degree is greater than the fourth similarity degree according to the second comparison result; if yes, determine that a
25 comparison of similarity degrees between the sample feature information corresponding to

the sample user and the reference feature information corresponding to each sample user is successful; otherwise, determine that the comparison of similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user is failed; and collect statistics on a ratio of the number of successful similarity degree comparisons, and determine that the at least two sample users meet the preset distinguishability condition when the ratio of the number is greater than the preset ratio value.

Optionally, as shown in FIG. 8, the apparatus further includes:

an acquisition module 740 configured to acquire a global user information database when the user to be authenticated does not belong to the similar user group, the global user information database including reference feature information and identifier information corresponding to each one of users in excess of a preset number;

a determining module 750 configured to determine reference feature information corresponding to the user to be authenticated in the global user information database according to identifier information corresponding to the user to be authenticated; and

a second authentication module 760 configured to authenticate the user to be authenticated according to the reference feature information corresponding to the user to be authenticated.

Optionally, the feature information includes at least one piece of the following information: a face feature, an iris feature, a fingerprint, and an eyeprint, and the identifier information includes at least one of an ID number, a communication number, a name, and predetermined identifier information.

In an embodiment, one or more embodiments of this specification further provide an apparatus for user authentication based on feature information, including:

a receiving module configured to receive an authentication request of a user to be

authenticated, the authentication request including identifier information of the user to be authenticated;

a second judgment module configured to judge whether the user to be authenticated belongs to a similar user group according to the identifier information of the user to be authenticated, wherein the similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition;

a calculation module configured to, if the user to be authenticated belongs to the similar user group, acquire feature information collected for the user to be authenticated, calculate a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculate a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user whose identifier information is the same as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

a determining module configured to determine that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree.

By using the apparatus according to one or more embodiments of this specification, it is first judged whether a user to be authenticated belongs to a similar user group, and if the user to be authenticated belongs to the similar user group, the user to be authenticated is authenticated according to reference feature information in the similar user group, wherein the similar user group includes at least two similar users, and the at least two similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition. It can be known that this technical solution can

implement authentication for the user to be authenticated by using the similar user group to which similar users meeting the preset similarity condition and the preset distinguishability condition belong. Therefore, the user to be authenticated can be distinguished from a similar user thereof, thus preventing misrecognition between multiple similar users (for example, faces of father and son, identical twins, and so on), and further improving an accuracy rate of the user authentication. In addition, compared with the existing art in which authentication for similar users is shielded, this technical solution greatly improves a coverage rate of the user authentication.

Those skilled in the art can understand that the apparatus for user authentication based on feature information in FIG. 7 and FIG. 8 can be used to implement the method for user authentication based on feature information described above, wherein the description of details should be similar to the description of the preceding method part. To avoid tediousness, details are not described here again.

Based on the same conception, one or more embodiments of this specification further provide an apparatus for user authentication based on feature information, as shown in FIG. 9. The apparatus for user authentication based on feature information may vary significantly due to different configurations or performance, and may include one or more processors 901 and a memory 902. One or more application programs or data may be stored in the memory 902. The memory 902 may support transient storage or persistent storage. The application program stored in the memory 902 may include one or more modules (not shown), and each module may include a series of computer executable instructions in the apparatus for user authentication based on feature information. Furthermore, the processor 901 may be configured to communicate with the memory 902, and execute a series of computer executable instructions in the memory 902 on the apparatus for user authentication based on feature information. The apparatus for user

authentication based on feature information may further include one or more power supplies 903, one or more wired or wireless network interfaces 904, one or more input/output interfaces 905, and one or more keyboards 906.

Specifically in this embodiment, the apparatus for user authentication based on feature
5 information includes a memory and one or more programs, wherein the one or more programs are stored in the memory and may include one or more modules; each module may include a series of computer executable instructions in the apparatus for user authentication based on feature information, and through configuration, one or more processors execute the one or more programs including following computer executable
10 instructions:

judging whether a user to be authenticated belongs to a similar user group, wherein the similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition; and

15 authenticating the user to be authenticated according to reference feature information in the similar user group if the user to be authenticated belongs to the similar user group.

Optionally, when the computer executable instructions are executed, the processor may further be enabled to perform the following operations:

the authenticating the user to be authenticated according to reference feature
20 information in the similar user group includes:

acquiring feature information collected for the user to be authenticated;

comparing the collected feature information with each piece of reference feature information in the similar user group to obtain a first comparison result; and

determining whether the user to be authenticated passes the authentication according to
25 the first comparison result.

Optionally, when the computer executable instructions are executed, the processor may further be enabled to perform the following operations:

acquiring identifier information of the user to be authenticated; and

judging whether the identifier information of the user to be authenticated matches
5 identifier information of a similar user in a pre-stored similar user group; if yes, determining that the user to be authenticated belongs to the similar user group; otherwise, determining that the user to be authenticated does not belong to the similar user group.

Optionally, the preset similarity condition includes: a similarity degree of the reference feature information reaches a preset threshold.

10 Optionally, the preset distinguishability condition includes: based on comparisons of similarity degrees between the sample feature information of a similar user and each piece of reference feature information in the similar user group to which the similar user belongs, a ratio of the number of successful similarity degree comparisons is greater than a preset ratio value.

15 Optionally, when the computer executable instructions are executed, the processor may further be enabled to perform the following operations:

calculating a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and
20 reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user whose identifier information is the same as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated;

correspondingly, determining that the user to be authenticated passes the authentication
25 if the first similarity degree is greater than the second similarity degree; and

determining that the user to be authenticated does not pass the authentication if the first similarity degree is not greater than the second similarity degree.

Optionally, when the computer executable instructions are executed, the processor may further be enabled to perform the following operations:

5 acquiring reference feature information and sample feature information corresponding to each one of at least two sample users, wherein the reference feature information of the at least two sample users meets the preset similarity condition;

 calculating, for any of the sample users, similarity degrees between the sample feature information corresponding to the sample user and the reference feature information
10 corresponding to each sample user;

 judging whether the at least two sample users meet the preset distinguishability condition according to the calculated similarity degrees; and

 adding the at least two sample users to the same similar user group when the at least two sample users meet the preset distinguishability condition.

15 Optionally, when the computer executable instructions are executed, the processor may further be enabled to perform the following operations:

 comparing a third similarity degree between the sample feature information corresponding to the sample user and the reference feature information corresponding to the sample user with a fourth similarity degree between the sample feature information
20 corresponding to the sample user and the reference feature information corresponding to the sample users other than the sample user, to obtain a second comparison result;

 judging whether the third similarity degree is greater than the fourth similarity degree according to the second comparison result;

 if yes, determining that a comparison of similarity degrees between the sample feature
25 information corresponding to the sample user and the reference feature information

corresponding to each sample user is successful; otherwise, determining that the comparison of similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user is failed; and

- 5 collecting statistics on a ratio of the number of successful similarity degree comparisons, and determining that the at least two sample users meet the preset distinguishability condition when the ratio of the number is greater than the preset ratio value.

Optionally, when the computer executable instructions are executed, the processor may
10 further be enabled to perform the following operations:

acquiring a global user information database when the user to be authenticated does not belong to the similar user group, the global user information database including reference feature information and identifier information corresponding to each one of users in excess of a preset number;

- 15 determining reference feature information corresponding to the user to be authenticated in the global user information database according to identifier information corresponding to the user to be authenticated; and

authenticating the user to be authenticated according to the reference feature information corresponding to the user to be authenticated.

- 20 Optionally, the feature information includes at least one piece of the following information: a face feature, an iris feature, a fingerprint, and an eyeprint, and the identifier information includes at least one of an ID number, a communication number, a name, and predetermined identifier information.

Specifically, in this embodiment, the apparatus for user authentication based on feature
25 information may further be configured such that one or more processors execute the one or

more programs including the following computer executable instructions:

receiving an authentication request of a user to be authenticated, the authentication request including identifier information of the user to be authenticated;

5 judging whether the user to be authenticated belongs to a similar user group according to the identifier information of the user to be authenticated, wherein the similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition;

if the user to be authenticated belongs to the similar user group, acquiring feature information collected for the user to be authenticated, calculating a first similarity degree
10 between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user whose identifier information is the same as that of the user to be authenticated, and the
15 second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

determining that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree.

One or more embodiments of this specification further provide a computer readable
20 storage medium. The computer readable storage medium stores one or more programs that include instructions. When executed by an electronic device including a plurality of application programs, the instructions can enable the electronic device to perform the foregoing method for user authentication based on feature information, and specifically perform the following operations:

25 judging whether a user to be authenticated belongs to a similar user group, wherein the

similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition; and

5 authenticating the user to be authenticated according to reference feature information in the similar user group if the user to be authenticated belongs to the similar user group.

One or more embodiments of this specification further provide another computer readable storage medium. The computer readable storage medium stores one or more programs that include instructions. When executed by an electronic device including a plurality of application programs, the instructions can enable the electronic device to
10 perform the foregoing method for user authentication based on feature information, and specifically perform the following operations:

receiving an authentication request of a user to be authenticated, the authentication request including identifier information of the user to be authenticated;

judging whether the user to be authenticated belongs to a similar user group according
15 to the identifier information of the user to be authenticated, wherein the similar user group includes at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition;

if the user to be authenticated belongs to the similar user group, acquiring feature information collected for the user to be authenticated, calculating a first similarity degree
20 between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user whose identifier information is the same as that of the user to be authenticated, and the
25 second similar user is a similar user whose identifier information is different from that of

the user to be authenticated; and

determining that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree.

The system, apparatus, modules or units illustrated in the foregoing embodiments
5 specifically can be implemented by a computer chip or an entity, or implemented by a product having a specific function. A typical implementation device is a computer. Specifically, for example, the computer can be a personal computer, a 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,
10 or a combination of any of these devices.

For ease of description, the apparatus is divided into various units based on functions, and the units are described separately. Definitely, during the implementation of one or more embodiments of this specification, functions of various units can also be implemented in one or more pieces of software and/or hardware.

15 Those skilled in the art should understand that one or more embodiments of this specification can be provided as a method, a system, or a computer program product. Therefore, one or more embodiments of this specification may be implemented as a complete hardware embodiment, a complete software embodiment, or an embodiment combining software and hardware. Moreover, one or more embodiments of this
20 specification can be in the form of a computer program product implemented on one or more computer usable storage media (including, but not limited to, a magnetic disk memory, a compact disk read-only memory (CD-ROM), an optical memory and the like) including computer usable program codes.

One or more embodiments of this specification are described with reference to
25 flowcharts and/or block diagrams of the method, device (system) and computer program

product according to one or more embodiments of this specification. It should be understood that computer program instructions can be used to implement each process and/or block in the flowcharts and/or block diagrams and combinations of processes and/or blocks in the flowcharts and/or block diagrams. These computer program instructions can be provided to a general-purpose computer, a special-purpose computer, an embedded processor, or a processor of another programmable data processing device to generate a machine, such that the instructions executed by a computer or a processor of another programmable data processing device generate an apparatus for implementing functions specified in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

The computer program instructions may also be stored in a computer readable memory that can guide the computer or another programmable data processing device to work in a specific manner, such that the instructions stored in the computer readable memory generate an article of manufacture including an instruction apparatus, and the instruction apparatus implements functions specified in one or more processes in the flowcharts and/or one or more blocks in the block diagrams.

These computer program instructions can also be loaded onto a computer or another programmable data processing device, such that a series of operation steps are performed on the computer or another programmable device to generate computer-implemented processing. Therefore, the instructions executed on the computer or another programmable device provide steps for implementing functions specified in one or more processes in the flowcharts and/or one or more blocks in the block diagrams.

In a typical configuration, the computing device includes one or more processors (CPU), an input/output interface, a network interface, and a memory.

The memory may include forms such as a volatile memory, a random access memory

(RAM) and/or a non-volatile memory in a computer readable medium, for example, a read-only memory (ROM) or a flash RAM. The memory is an example of the computer readable medium.

The computer readable medium includes non-volatile and volatile media as well as
5 movable and non-movable media, and can implement information storage by means of any method or technology. Information may be a computer readable instruction, a data structure, and a module of a program or other data. An example of a storage medium of a computer includes, but is not limited to, a phase change memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), other types of
10 RAMs, a ROM, an electrically erasable programmable read-only memory (EEPROM), a flash memory or other memory technologies, a 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 media, and can be used to store information accessible to the computing device. According to the definition in this text, the
15 computer readable medium does not include transitory media, such as modulated data signals and carriers.

It should be further noted that, the terms "include", "comprise" or any other variations thereof are intended to cover a non-exclusive inclusion, so that a process, method, article or device including a series of elements not only includes the elements, but also includes
20 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 the process, method, article or device including the element further has other identical elements.

Those skilled in the art should understand that one or more embodiments of this
25 specification can be provided as a method, a system, or a computer program product.

Therefore, one or more embodiments of this specification can be implemented as a complete hardware embodiment, a complete software embodiment, or an embodiment combining software and hardware. Moreover, one or more embodiments of this specification may be in the form of a computer program product implemented on one or
5 more computer usable storage media (including, but not limited to, a magnetic disk memory, a CD-ROM, an optical memory, and the like) including computer usable program codes.

One or more embodiments of this specification can be described in a general context of a computer executable instruction executed by a computer, for example, a program module.

10 Generally, the program module includes a routine, a program, an object, an assembly, a data structure, and the like for executing a specific task or implementing a specific abstract data type. One or more embodiments of this specification can also be implemented in distributed computing environments. In the distributed computing environments, a task is executed by using remote processing devices connected through a communications
15 network. In the distributed computing environments, the program module may be located in local and remote computer storage media including a storage device.

The embodiments in this specification are described progressively. For identical or similar parts of the embodiments, reference may be made to each other. Each embodiment focuses on a difference from other embodiments. Especially, the system embodiment is
20 basically similar to the method embodiment, and therefore is described in a relatively simple manner. For related parts, reference may be made to the partial description of the method embodiment.

The above description is merely one or more embodiments of this specification, and is not used to limit one or more embodiments of this specification. For those skilled in the art,
25 one or more embodiments of this specification can have various alterations and changes.

Any modification, equivalent replacement, improvement and the like made without departing from the spirit and principle of one or more embodiments of this specification should fall in the scope of the claims of one or more embodiments of this specification.

CLAIMS

1. A method for user authentication based on feature information, comprising:

judging whether a user to be authenticated belongs to a similar user group, wherein the similar user group comprises at least two similar users, and the similar users are users
5 whose reference feature information meets a preset similarity condition and a preset distinguishability condition; and

authenticating the user to be authenticated according to reference feature information in the similar user group if the user to be authenticated belongs to the similar user group.

2. The method according to claim 1, wherein the authenticating the user to be
10 authenticated according to reference feature information in the similar user group comprises:

acquiring feature information collected for the user to be authenticated;

comparing the collected feature information with each piece of reference feature information in the similar user group to obtain a first comparison result; and

15 determining whether the user to be authenticated passes the authentication according to the first comparison result.

3. The method according to claim 1, wherein the judging whether a user to be authenticated belongs to a similar user group comprises:

acquiring identifier information of the user to be authenticated; and

20 judging whether the identifier information of the user to be authenticated matches identifier information of a similar user in a pre-stored similar user group; if yes, determining that the user to be authenticated belongs to the similar user group; otherwise, determining that the user to be authenticated does not belong to the similar user group.

4. The method according to any of claims 1 to 3, wherein the preset similarity
25 condition comprises: a similarity degree of the reference feature information reaches a

preset threshold.

5 5. The method according to any of claims 1 to 3, wherein the preset distinguishability condition comprises: based on comparisons of similarity degrees between the sample feature information of the similar user and each piece of reference feature information in the similar user group to which the similar user belongs, a ratio of the number of successful similarity degree comparisons is greater than a preset ratio value.

6. The method according to claim 2, wherein the comparing the collected feature information with each piece of reference feature information in the similar user group to obtain a first comparison result comprises:

10 calculating a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated;

correspondingly, the determining whether the user to be authenticated passes the authentication according to the first comparison result comprises:

20 determining that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree; and

determining that the user to be authenticated does not pass the authentication if the first similarity degree is not greater than the second similarity degree.

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

25 acquiring reference feature information and sample feature information corresponding to each one of at least two sample users, wherein the reference feature information of the at

least two sample users meets the preset similarity condition;

calculating, for any of the sample users, similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user;

5 judging whether the at least two sample users meet the preset distinguishability condition according to the calculated similarity degrees; and

adding the at least two sample users to the same similar user group when the at least two sample users meet the preset distinguishability condition.

8. The method according to claim 7, wherein the judging whether the at least two
10 sample users meet the preset distinguishability condition according to the calculated similarity degrees comprises:

comparing a third similarity degree between the sample feature information corresponding to the sample user and the reference feature information corresponding to the sample user with a fourth similarity degree between the sample feature information
15 corresponding to the sample user and the reference feature information corresponding to the sample users other than the sample user, to obtain a second comparison result;

judging whether the third similarity degree is greater than the fourth similarity degree according to the second comparison result;

if yes, determining that a comparison of similarity degrees between the sample feature
20 information corresponding to the sample user and the reference feature information corresponding to each sample user is successful; otherwise, determining that the comparison of similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user is failed; and

25 collecting statistics on a ratio of the number of successful similarity degree

comparisons, and determining that the at least two sample users meet the preset distinguishability condition when the ratio of the number is greater than the preset ratio value.

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

5 acquiring a global user information database when the user to be authenticated does not belong to the similar user group, the global user information database comprising reference feature information and identifier information corresponding to each one of users in excess of a preset number;

 determining reference feature information corresponding to the user to be
10 authenticated in the global user information database according to identifier information corresponding to the user to be authenticated; and

 authenticating the user to be authenticated according to the reference feature information corresponding to the user to be authenticated.

10. The method according to claim 3, wherein the feature information comprises at
15 least one piece of the following information: a face feature, an iris feature, a fingerprint, and an eyeprint, and the identifier information comprises at least one of an ID number, a communication number, a name, and predetermined identifier information.

11. A method for user authentication based on feature information, comprising:

 receiving an authentication request of a user to be authenticated, the authentication
20 request comprising identifier information of the user to be authenticated;

 judging whether the user to be authenticated belongs to a similar user group according to the identifier information of the user to be authenticated, wherein the similar user group comprises at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition;

25 if the user to be authenticated belongs to the similar user group, acquiring feature

information collected for the user to be authenticated, calculating a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

determining that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree.

12. An apparatus for user authentication based on feature information, comprising:

a first judgment module configured to judge whether a user to be authenticated belongs to a similar user group, wherein the similar user group comprises at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition; and

a first authentication module configured to authenticate the user to be authenticated according to reference feature information in the similar user group if the user to be authenticated belongs to the similar user group.

13. The apparatus according to claim 12, wherein the first authentication module comprises:

a first acquisition unit configured to acquire feature information collected for the user to be authenticated;

a comparison unit configured to compare the collected feature information with each piece of reference feature information in the similar user group to obtain a first comparison result; and

a determining unit configured to determine whether the user to be authenticated passes the authentication according to the first comparison result.

14. The apparatus according to claim 12, wherein the first judgment module comprises:

5 an identifier information acquisition unit configured to acquire identifier information of the user to be authenticated; and

 a first judgment unit configured to judge whether the identifier information of the user to be authenticated matches identifier information of a similar user in a pre-stored similar user group; if yes, determine that the user to be authenticated belongs to the similar user group; otherwise, determine that the user to be authenticated does not belong to the similar user group.

15 15. The apparatus according to claim 13, wherein the comparison unit is configured to calculate a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculate a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

20 correspondingly, the determining unit is configured to determine that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree; and determine that the user to be authenticated does not pass the authentication if the first similarity degree is not greater than the second similarity degree.

25 16. The apparatus according to claim 12, further comprising a creation module configured to create the similar user group;

wherein the creation module comprises:

a second acquisition unit configured to acquire reference feature information and sample feature information corresponding to each one of at least two sample users, wherein the reference feature information of the at least two sample users meets the preset
5 similarity condition;

a calculation unit configured to calculate, for any of the sample users, similarity degrees between the sample feature information corresponding to the sample user and the reference feature information corresponding to each sample user;

a second judgment unit configured to judge whether the at least two sample users
10 meet the preset distinguishability condition according to the calculated similarity degrees; and

an adding unit configured to add the at least two sample users to the same similar user group when the at least two sample users meet the preset distinguishability condition.

17. An apparatus for user authentication based on feature information, comprising:

15 a receiving module configured to receive an authentication request of a user to be authenticated, the authentication request comprising identifier information of the user to be authenticated;

a second judgment module configured to judge whether the user to be authenticated belongs to a similar user group according to the identifier information of the user to be
20 authenticated, wherein the similar user group comprises at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition;

a calculation module configured to, if the user to be authenticated belongs to the similar user group, acquire feature information collected for the user to be authenticated,
25 calculate a first similarity degree between the collected feature information and reference

feature information corresponding to a first similar user in the similar user group, and calculate a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

a determining module configured to determine that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree.

18. An apparatus for user authentication based on feature information, comprising:

a processor; and

a memory configured to store computer executable instructions, wherein the processor is enabled to perform the following steps when the computer executable instructions are executed:

judging whether a user to be authenticated belongs to a similar user group, wherein the similar user group comprises at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition; and

authenticating the user to be authenticated according to reference feature information in the similar user group if the user to be authenticated belongs to the similar user group.

19. An apparatus for user authentication based on feature information, comprising:

a processor; and

a memory configured to store computer executable instructions, wherein the processor is enabled to perform the following steps when the computer executable instructions are executed:

receiving an authentication request of a user to be authenticated, the authentication

request comprising identifier information of the user to be authenticated;

judging whether the user to be authenticated belongs to a similar user group according to the identifier information of the user to be authenticated, wherein the similar user group comprises at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition;

if the user to be authenticated belongs to the similar user group, acquiring feature information collected for the user to be authenticated, calculating a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and reference feature information corresponding to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

determining that the user to be authenticated passes the authentication if the first similarity degree is greater than the second similarity degree.

20. A storage medium for storing computer executable instructions, wherein the following processes are implemented when the computer executable instructions are executed:

judging whether a user to be authenticated belongs to a similar user group, wherein the similar user group comprises at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition; and

authenticating the user to be authenticated according to reference feature information in the similar user group if the user to be authenticated belongs to the similar user group.

21. A storage medium for storing computer executable instructions, wherein the following processes are implemented when the computer executable instructions are executed:

receiving an authentication request of a user to be authenticated, the authentication
5 request comprising identifier information of the user to be authenticated;

judging whether the user to be authenticated belongs to a similar user group according to the identifier information of the user to be authenticated, wherein the similar user group comprises at least two similar users, and the similar users are users whose reference feature information meets a preset similarity condition and a preset distinguishability condition;

10 if the user to be authenticated belongs to the similar user group, acquiring feature information collected for the user to be authenticated, calculating a first similarity degree between the collected feature information and reference feature information corresponding to a first similar user in the similar user group, and calculating a second similarity degree between the collected feature information and reference feature information corresponding
15 to a second similar user in the similar user group, wherein the first similar user is a similar user having the same identifier information as that of the user to be authenticated, and the second similar user is a similar user whose identifier information is different from that of the user to be authenticated; and

determining that the user to be authenticated passes the authentication if the first
20 similarity degree is greater than the second similarity degree.