IDENTITY AUTHENTICATION METHOD AND APPARATUS, TERMINAL AND SERVER

Technical Field

The present application relates to the field of communication technologies, and in particular, to identity authentication methods and apparatuses, terminals and servers.

Background

With the growth of intelligent terminals and the development of network applications, a user may access various types of network applications, such as social-type instant communication applications and shopping-type applications, through various types of application client terminals that are installed on a terminal. During an access, an identity of a user generally needs to be authenticated, such that the user is allowed to use various application functions after the authentication of the identity is successful.

In existing technologies, a user generally needs to enter an authentication password in an authentication interface during identity authentication, and a server confirms that the user passes the identity authentication upon verifying that the entered authentication password is the same as an authentication password during user registration. However, an authentication password is generally a simple combination of numerals and letters, and is easily stolen by a malicious third party. Therefore, existing methods of identity authentication mode are relatively poor in reliability and are prone to causing user information to be stolen, thus resulting in the poor security of authentication.

Summary

The present application provides a method, an apparatus, a terminal, and a server for identity authentication, to solve the problems of poor reliability and low security of the identity authentication methods in the existing technologies.

According to a first aspect of embodiments of the present application, an identity authentication method is provided. The method includes:

receiving dynamic human face authentication prompt information sent by a server when an authentication of an identity of a user is performed;

obtaining gesture recognition information of the dynamic human face authentication prompt information by recognizing a facial gesture presented by the user; and

sending the gesture recognition information to the server to enable the server to confirm that the authentication of the identity of the user is successful in response to verifying that the gesture recognition information is consistent with the dynamic human face authentication prompt information.

According to a second aspect of the embodiments of the present application, an identity authentication method is provided. The method includes:

sending dynamic human face authentication prompt information to a terminal when an authentication of an identity of a user is performed;

receiving gesture recognition information sent by the terminal, the gesture recognition information being gesture recognition information obtained by the terminal through recognizing a facial gesture that is presented by the user according to the dynamic human face authentication prompt information; and

determining that the authentication of the identity of the user is successful upon verifying that the gesture recognition information is consistent with the dynamic human face

authentication prompt information.

According to a third aspect of the embodiments of the present application, an identity authentication apparatus is provided. The apparatus includes:

a receiving unit configured to receive dynamic human face authentication prompt information sent by a server when an authentication of an identity of a user is performed;

a recognition unit configured to obtain gesture recognition information of the dynamic human face authentication prompt information by recognizing a facial gesture that is presented by the user; and

a sending unit configured to send the gesture recognition information to the server to enable the server to confirm that the authentication of the identity of the user is successful upon verifying that the gesture recognition information is consistent with the dynamic human face authentication prompt information.

According to a fourth aspect of the embodiments of the present application, an identity authentication apparatus is provided. The apparatus includes:

a sending unit configured to send dynamic human face authentication prompt information to a terminal when an authentication of an identity of a user is performed;

a receiving unit configured to receive gesture recognition information sent by the terminal, the gesture recognition information being gesture recognition information obtained by the terminal through recognizing a facial gesture that is presented by the user according to the dynamic human face authentication prompt information; and

a determination unit configured to determine that the authentication of the identity of the user is successful upon verifying that the gesture recognition information is consistent with the dynamic human face authentication prompt information.

According to a fifth aspect of the embodiments of the present application, a terminal is

provided, which includes:

processor(s); and memory configured to store instructions executable by the processor(s);

wherein the processor(s) is/are configured to:

receive dynamic human face authentication prompt information sent by a server when an authentication of an identity of a user is performed;

obtain gesture recognition information of the dynamic human face authentication prompt information by recognizing a facial gesture that is presented by the user; and

send the gesture recognition information to the server to enable the server to confirm that the authentication of the identity of the user is successful upon verifying that the gesture recognition information is consistent with the dynamic human face authentication prompt information.

According to a sixth aspect of the embodiments of the present application, a server is provided, which includes:

processor(s); and memory configured to store instructions executable by the processor(s);

wherein the processor(s) is/are configured to:

send dynamic human face authentication prompt information to a terminal when an authentication of an identity of a user is performed;

receive gesture recognition information sent by the terminal, the gesture recognition information being gesture recognition information obtained by the terminal through recognizing a facial gesture that is presented by the user according to the dynamic human face authentication prompt information; and

determine that the authentication of the identity of the user is successful upon verifying that the gesture recognition information is consistent with the dynamic face authentication prompt information.

In the embodiments of the present application, when identity authentication is performed for a user, a server sends dynamic authentication prompt information to a terminal. The terminal obtains gesture recognition information of the dynamic human face authentication prompt information by recognizing a facial gesture that is presented by the user, and sends the gesture recognition information to the server. The server determines that the authentication of the identity of the user is successful upon verifying that the gesture recognition information is consistent with the dynamic human face authentication prompt information. Using the embodiments of the present application, authentication having a high security can be performed on a user identity using dynamic human face authentication. As compared with existing authentication methods that use an authentication password, authentication information will not be stolen by a malicious third party, thus improving the reliability of authentication. Moreover, a user may be recognized as a live user via dynamic human face authentication, thereby further improving the accuracy of identity authentication and reducing potential security risks during a process of authentication.

The invention is defined in the independent claims 1, 8 and 13.

Brief Description of the Drawings

FIG. 1 is a schematic diagram of an identity authentication scenario according to an embodiment of the present application.

FIG. 2A is a flowchart of an example identity authentication method according to the present application.

FIG. 2B is a flowchart of another example identity authentication method according to the present application.

FIG. 3A is a flowchart of another example identity authentication method according to the present application.

FIG. 3B is a schematic diagram of a human head gesture during human face authentication in an embodiment of the present application.

FIG. 4A is a flowchart of another example identity authentication method according to the present application.

FIG. 4B and FIG. 4C are schematic diagrams of facial key points in an embodiment of the present application.

FIG. 5 is a structural diagram illustrating hardware of a device where an identity authentication apparatus according to the present application is located.

FIG. 6 is a block diagram of an example identity authentication apparatus according to the present application.

FIG. 7 is a block diagram of another example identity authentication apparatus according to the present application.

The invention is defined in the independent claims 1, 8 and 13.

Detailed Description

Exemplary embodiments will be described herein in detail, and examples thereof are represented in accompanying drawings. When the following description involves the accompanying drawings, identical numbers in different accompanying drawings represent identical or similar elements, unless specified otherwise. Implementations described in the following exemplary embodiments do not represent all implementations that are consistent

with the present application. On the contrary, they are merely examples of apparatuses and methods consistent with some aspects of the present application as described in detail in the appended claims.

Terms used in the present application are merely used for describing specific embodiments rather than limiting the present application. Singular forms "a", "the", and "said" that are used in the present application and the appended claims are also intended to include plural forms, unless the context clearly indicates other meanings. It should further be understood that, the term "and/or" used herein refers to and includes any or all possible combinations of one or more associated items listed.

It should be understood that, although terms such as "first", "second", and "third" may be used to describe various types of information in the present application, those pieces of information are not limited by these terms. These terms are merely used for distinguishing information of the same type from each other. For example, without departing from the scope of the present application, first information may also be referred to as second information, and similarly, second information may alternatively be referred to as first information. Depending on the context, "if" as used herein may be interpreted as "when", "while", or "in response to determining that".

In an Internet-based communication scenario, a user may access various types of network applications through various types of application terminals installed on a terminal thereof. During an access process, an identity of the user generally needs to be authenticated. However, in existing technologies, an identity of a user is generally authenticated via an authentication password, and the authentication password is generally a simple combination of numerals and letters, which is easily stolen by a malicious third party. Therefore, existing identity authentication methods are relatively poor in reliability

and have a poor security. Accordingly, referring to FIG. 1, which is a schematic diagram of an application scenario for implementing identity authentication according to an embodiment of the present application, identity authentication for a user is completed through interactions between a terminal held thereby and a server. Communications between the terminal and the server may be completed based on a network. The network includes various types of wireless networks or wired networks, which is not limited in the embodiments of the present application. The terminal may be a mobile phone, a tablet computer, a personal computer, etc. In the application scenario as shown in FIG. 1, two databases may be deployed in the server, which are a human facial feature information database and a dynamic human face authentication prompt information database respectively.

In a face registration phase, the terminal may acquire human facial feature information of a registered user, which is sent to the server. The server stores the human facial feature information of the registered user into the facial feature information database. In an identity authentication phase, human face authentication may be performed first. At this point, a user sends acquired human facial feature information to the server. Upon verifying that the human facial feature information matches human facial feature information of the user that is stored in the facial feature information data, the server may preliminarily determine that an identity authentication is currently performed on the user himself/herself. Dynamic human face authentication is then performed. At this point, the server may return dynamic human face authentication prompt information acquired from the dynamic human face authentication prompt information database to the user. The terminal recognizes a human facial gesture presented by the user to obtain gesture recognition information of the dynamic human face authentication prompt information, and sends the gesture recognition

information to the server. Upon verifying that the gesture recognition information is consistent with the dynamic human face authentication prompt information, the server knows that the current user to be authenticated is a live user, thereby finally determining that the identity authentication of the user is successful. For ease of description, in the embodiments of the present application, human facial feature information of a user acquired in the face registration phase is referred to as second human facial feature information, and human facial feature information of the user acquired in the face authentication phase is referred to as first human facial feature information. The embodiments of the present application are described in detail hereinafter.

FIG. 2A is a flowchart of an embodiment of an identity authentication method according to the present application. This embodiment is described from the perspective of a terminal that implements an identity authentication.

Step 201 receives dynamic human face authentication prompt information sent by a server during identity authentication of a user.

In this embodiment of the present application, the server may randomly extract dynamic human face authentication prompt information from dynamic human face authentication prompt information data and returns the dynamic human face authentication prompt information to the terminal. The dynamic human face authentication prompt information may include at least one type of the following information: expression action prompt information, such as closing eye(s), opening a mouth, or turning a head; or voice read prompt information, such as making a payment of 20 dollars.

Optionally, prior to receiving the dynamic human face authentication prompt information from the server, the terminal may first acquire human facial feature information of the user, and use the human facial feature information acquired during the identity

authentication as first human facial information of the user. After the first human facial feature information of the user is sent to the server, the server sends the dynamic human face authentication prompt information to the terminal when verifying that the first human facial feature information matches the second facial feature information that is stored.

When acquiring human facial feature information of the user, the terminal may start an imaging device integrated thereon, such as a camera, to detect a human face of the user, and track the human face of the user when the human face is detected. During human face tracking, the terminal acquires human face images according to a preset time interval, determines whether a respective face image fulfills a preset feature extraction condition for each acquired face image, and extracts human facial feature information of the user from that face image if that face image fulfills the feature extraction condition.

After receiving the first human facial feature information of the user, the server may search the facial feature information database based on a user name of the user to obtain second facial feature information corresponding to the user name, and then compares the first human facial feature information and the second human facial feature information using a predefined comparison approach. If a feature comparison value falls within a preset similarity range, a determination may be made that the first human facial feature information matches the second facial feature information. In response to determining that the first human facial feature information matches the second human facial feature information, a determination can be made that human face authentication is successful for the user. In this case, the server sends the dynamic human face authentication prompt information to the terminal.

Step 202 obtains gesture recognition information of the dynamic human face authentication prompt information by recognizing a facial gesture presented by the user.

In this embodiment of the present application, after receiving the dynamic human face authentication prompt information, the terminal displays the dynamic human face authentication prompt information in an identity authentication interface. The user may present a corresponding human facial gesture according to the information. When recognizing the human facial gesture, the terminal may track the human face of the user to obtain face tracking information. The human face tracking information may include at least one of facial key point position information and human head gesture information. The terminal then obtains gesture recognition information of the user by analyzing the human face tracking information. For example, through the facial key point position information, whether the user closes eye(s) or opens a mouth according to the expression action prompt information may be known, or a mouth shape of the user when reading the voice read prompt information may be known (a correspondence relationship between pronunciation and a mouth shape of each word exists, and gesture recognition information of the user can be determined based on the mouth shape). Furthermore, whether the user turns his/her head, lowers the head, etc., may be known through the head gesture information.

Step 203 sends the gesture recognition information to the server to enable the server to confirm that the identity authentication is successful for the user, upon verifying that the gesture recognition information is consistent with the dynamic human face authentication prompt information.

The server may need to perform identity authentication for multiple users at one time. If different pieces of dynamic authentication prompt information are sent to different users, the server may record a correspondence relationship between a user name of the user and the dynamic human face authentication prompt information after sending the dynamic human face authentication prompt information to the terminal at step 201. At this step,

after the terminal sends the gesture recognition information to the server, the server acquires corresponding dynamic human face authentication prompt information according to the user name of the user and verifies that the gesture recognition information is consistent with the dynamic human face authentication prompt information. This indicates that the user is a live user, and in this case, the identity authentication is determined to be successful for the user.

In addition, if the dynamic human face authentication prompt information at step 201 is voice read prompt information, the terminal may also obtain audio information of the user in addition to the mouth shape of the user. Through voice recognition of the audio information, voice information read by the user is obtained, such that the server may compare whether the voice information is consistent with the voice read prompt information, and determine that the identity authentication is successful for the user if they are consistent.

FIG. 2B is a flowchart of another embodiment of an identity authentication method according to the present application. This embodiment is described from the perspective of a server that implements identity authentication:

Step 211 sends dynamic human face authentication prompt information to a terminal when an identity authentication of a user is performed.

Step 212 receives gesture recognition information sent by the terminal, the gesture recognition information being gesture recognition information obtained by the terminal through recognizing a human facial gesture that is presented by the user according to the dynamic human face authentication prompt information.

Step 213 determines that the identity authentication of the user is successful upon verifying that the gesture recognition information is consistent with the dynamic human face

authentication prompt information.

It should be noted that, the only difference between the process of identity authentication as shown in FIG. 2B and the process of identity authentication as shown in FIG. 2A is a difference in entities of execution. Specifically, FIG. 2A is described from the perspective of a terminal, while FIG. 2B is described from the perspective of a server. Therefore, related processes of implementations in the embodiment of FIG. 2B may be referenced to the above description of FIG. 2A, and are not repeatedly described herein.

As can be seen from the foregoing embodiment, this embodiment can perform user identity authentication having a high security by means of dynamic human face authentication. Compared with existing authentication methods using an authentication password, authentication information will not be stolen by a malicious third party, thus improving the reliability of authentication. Moreover, a user may be recognized as a live user via dynamic human face authentication, thereby further improving the accuracy of identity authentication and reducing potential security risks during authentication.

FIG. 3A is another embodiment of an identity authentication method according to the present application. This embodiment illustrates a process of human face registration in detail.

Step 301: A user registers with a server through a terminal.

Step 302: The terminal tracks the human face of the user when the human face of the user is detected.

Generally, an imaging device, such as a camera, is integrated in the terminal. In this embodiment, the imaging device may be set to automatically start to detect a human face of the user by default during user registration. Generally, the user may hold the terminal with a hand to align the imaging device with the face of the user. When the face is detected

through the imaging device, the terminal may track the face of the user according to a human face tracking algorithm. It should be noted that this embodiment of the present application may employ various types of existing face tracking algorithms, which are not described in detail herein.

Step 303: The terminal acquires a face image according to a preset time interval during face tracking.

During face tracking, the terminal acquires face images according to a preset time interval using the imaging device. The time interval is set to avoid extraction of face images that are substantially the same. For example, the preset time interval may be 3 seconds.

Step 304: A determination is made as to whether a resolution of the face image meets a preset resolution threshold. If affirmative, step 305 is performed. Otherwise, the current process is ended.

A resolution of the face image acquired at step 303 may be examined first to eliminate face image(s) having insufficient resolution. In this case, the terminal may invoke a preset fuzzy determination function to determine whether the resolution of the face image meets the resolution threshold. A fuzzy determination function in an existing image recognition processing technology may be used for this fuzzy determination function, which is not limited in this embodiment of the present application. For a face image satisfying the resolution threshold, step 305 is performed. A face image that does not satisfy the resolution threshold is directly discarded, and step 303 is then returned.

Step 305: The terminal extracts head gesture information from the face image.

After determining that the acquired face image is a clear face image at step 304, the terminal extracts head gesture information from the face image. FIG. 3B shows a schematic diagram of a head gesture in an embodiment of the present application. The head gesture

information in this embodiment may include at least one of the following angles: a head lowering/raising angle, a face turning angle, and a head leaning angle.

Step 306: The terminal determines whether each angle included in the head gesture information falls within a respective preset angle range. If yes, step 307 is performed. Otherwise, the current process is ended.

In this embodiment of the present application, a determination may be made as to whether the face image is a front face image of the user through the head gesture information. At this point, the terminal may determine whether each angle included in the head gesture information falls within a respective preset angle range. For example, a preset angle range is 0 to 10 degrees. For a face image corresponding to head gesture information of which a determination result is positive, step 307 is performed. A face image corresponding to head gesture information of which a determination result is negative is directly discarded, and step 303 is then returned.

Step 307: The terminal extracts information of facial feature(s) of the user from the face image.

In this embodiment of the present application, a Linear Back Projection (LBP) feature extraction algorithm may be employed to extract facial feature vector value(s) from the face image as the information of the facial feature(s) of the user. Apparently, this embodiment of the present application does not impose any limitations on a specific algorithm for facial feature extraction. Any facial feature extraction algorithm used in any existing image processing technology may be applicable to this embodiment of the present application, such as a Gabor feature extraction algorithm in windowed Fourier transform, etc.

To guarantee the accuracy of face authentication in the subsequent phase of identity authentication, facial feature information of a user may be extracted from multiple face

images for this same registered user during the phase of face registration. The number of face images may be preset, five, for example. Correspondingly, according to the set number of face images, the foregoing step 303 to step 307 may be performed repeatedly to obtain a number of face images that meets the preset number, and to extract facial feature information therefrom.

Step 308: The terminal sends the information of the facial feature(s) to the server.

Step 309: The server stores correspondence relationship(s) between a user name of the registered user and the facial feature(s), and the current process is ended.

In this embodiment, after receiving the information of the facial feature(s) from the terminal, the server may store the correspondence relationship(s) between the user name of the registered user and the facial feature(s) in the facial feature information database, and store correspondence relationships between the user name and information of multiple facial features upon receiving the information of the multiple facial features.

FIG. 4A is another embodiment of an identity authentication method according to the present application. This embodiment describes a process of authenticating an identity of a user in detail, based on the process of face registration as shown in FIG. 3.

Step 401: Identity authentication of a user is started.

Step 402: A terminal acquires first facial feature information of the user.

During identity authentication, the terminal acquires the facial feature information of the user using an approach that is the same as that of acquiring facial feature information in the process of face registration as shown in FIG. 3 above, and is specifically the same as step 302 to step 307 as shown in FIG. 3. Details thereof are not repeatedly described herein.

At this step, the terminal may acquire at least one piece of first facial feature information.

Step 403: The terminal sends the first facial feature information of the user to a server.

Step 404: The server verifies whether the first facial feature information matches second facial feature information of the user that is stored. If affirmative, step 405 is performed. Otherwise, the current process is ended.

In this embodiment of the present application, after receiving the first facial feature information of the user, the server may search the facial feature information database based on a user name of the user to obtain second facial feature information corresponding to the user name, and then compare the first facial feature information and the second facial feature information in a preset comparison manner. If a feature comparison value falls within a preset similarity range, a determination can be made that the first facial feature information matches the second facial feature information.

The facial feature information in this embodiment of the present application is said to be a facial feature vector extracted via the LBP algorithm as an example.

In one instance, a comparison of Euclidean distances may be used for comparing the first facial feature information and the second facial feature. In this case, a sum of squares of a difference between a second facial feature vector and a first facial feature vector is calculated. If the sum of squares is less than a preset threshold, a determination can be made that the identity authentication is performed on the user himself/herself.

In another instance, a comparison of cosine distances may be used for comparing the first facial feature information and the second facial feature. If a first facial feature vector is V1 and a second facial feature vector is V2, the following formula value may be calculated: V2*V1 / (|V1|*|V2|). If the formula value is greater than a preset threshold, a determination can be made that the identity authentication is performed on the user himself/herself.

Step 405: The server sends dynamic face authentication prompt information to the terminal.

In response to verifying that the first facial feature information matches the second facial feature information, the server confirms that the identity authentication is performed on the user himself/herself, and starts to perform a process of dynamic face authentication at this point. The server may randomly extract a piece of dynamic face authentication prompt information from the dynamic face authentication prompt information database.

In this embodiment, the dynamic face authentication prompt information may include expression action prompt information or voice read prompt information. An action prompted by expression action prompt information is generally an action that a user can easily present through a facial gesture, for example, opening a mouth, closing eye(s), turning a head, etc. For voice read prompt information, the information is generally short, such that the user can easily read it aloud during authentication, and the terminal can easily recognize a facial gesture of the user when the user reads it out.

Step 406: The terminal obtains face tracking information by tracking a face of the user.

After receiving the dynamic face authentication prompt information, the terminal may output the dynamic face authentication prompt information on an authentication interface. The user may present a corresponding facial gesture according to the information. During presentation, the terminal acquires face tracking information of the user through a face tracking algorithm. The face tracking information may include at least one type of the following information: facial key point position information and head gesture information.

Step 407: The terminal analyzes the face tracking information to obtain gesture recognition information of the user.

For example, if the dynamic face authentication prompt information is "open a mouth", the user correspondingly makes an action of opening the mouth. The terminal may obtain facial key point position information, which is specifically key point position information of the mouth, by tracking the face of the user. FIG. 4B and FIG. 4C are schematic diagrams of facial key point position information in this embodiment of the present application. FIG. 4B shows extracted information of key point position(s) of a mouth of a user in a normal state. FIG. 4C shows extracted information of key point position(s) of the mouth of the user after the user presents a gesture of opening the mouth. By comparing respective extracted information of the key point position(s) in FIG. 4B and FIG. 4C, i.e., by comparing respective coordinate distances between upper and lower key point positions of the mouth, gesture recognition information of the user can be obtained as "open a mouth".

In another example, if the dynamic face authentication prompt information is "turn a head", the user correspondingly makes an action of turning the head. The terminal may obtain head gesture information, which specifically may include three angles as shown in FIG. 3B, by tracking the face of the user. If angular values of the three angles meet respective angle value ranges defined by "turn a head", gesture recognition information of the user can be obtained as "turn the head".

Step 408: The terminal sends the gesture recognition information to the server.

Step 409: The server verifies whether the gesture recognition information is consistent with the dynamic face authentication prompt information. If affirmative, step 410 is executed. Otherwise, the current process is ended.

Step 410: The server determines that the identity authentication for the user is successful, and the current process is ended.

As can be seen from the above embodiment, this embodiment combines face authentication with dynamic authentication to perform a highly secure authentication for an identity of a user, and can preliminarily verify whether it is the user himself/herself via the face authentication. Compared with existing authentication methods using an authentication password, authentication information is not easily stolen by a malicious third party, thus improving the reliability of authentication. Moreover, after the user is confirmed, the user can be recognized as a live user through the dynamic face authentication, thereby further improving the accuracy of identity authentication and reducing potential security risks during authentication.

Corresponding to the embodiments of the identity authentication methods in the present application, the present application further provides embodiments of an apparatus, a terminal, and a server for identity authentication.

An embodiment of an identity authentication apparatus in the present application may be individually applied to a terminal and a server. An apparatus embodiment may be implemented by software, or may be implemented by hardware or a combination of software and hardware. A software implementation is used as an example. As a logical apparatus, the apparatus is formed by processor(s) of a device in which the apparatus is located to read corresponding computer program instructions from a non-volatile storage into memory for running. FIG. 5 shows a hardware structural diagram of a device where an example identity authentication apparatus is located according to the present application from the perspective of hardware level. In addition to processor(s), memory, a network interface, and a non-volatile storage as shown in FIG. 5, the device where the apparatus is located may generally include other additional hardware components according to actual

functions of the device. For example, a terminal may include a camera, a touch screen, a communication component, etc. A server may include a forward chip responsible for processing packets, etc.

FIG. 6 shows a block diagram of an embodiment of an identity authentication apparatus according to the present application. The identity authentication apparatus may be applied on a terminal. The apparatus includes a receiving unit 610, a recognition unit 620, and a sending unit 630.

The receiving unit 610 is configured to receive dynamic face authentication prompt information sent by a server during an identity authentication of a user.

The recognition unit 620 is configured to obtain gesture recognition information of the dynamic face authentication prompt information by recognizing a facial gesture presented by the user.

The sending unit 630 is configured to send the gesture recognition information to the server to enable the server to confirm that the identity authentication of the user is successful upon verifying that the gesture recognition information is consistent with the dynamic face authentication prompt information.

In an optional implementation, the recognition unit 620 may include (not shown in FIG. 6):

a face information obtaining subunit configured to obtain face tracking information by tracking a face of the user when the user presents a facial gesture according to the dynamic face authentication prompt information; and

a face information analysis subunit configured to analyze the face tracking information to obtain gesture recognition information of the user.

The face information analysis subunit may be specifically configured to obtain

expression gesture recognition information of the user by analyzing facial key point position information when the face tracking information is the facial key point position information, or obtain head turning recognition information of the user by analyzing head gesture information when the face tracking information is the head gesture information.

The dynamic face authentication prompt information may include at least one type of the following information: expression action prompt information, or voice read prompt information.

In another optional implementation, the apparatus may further include (not shown in FIG. 6) an acquisition unit configured to acquire facial feature information of the user, and use the facial feature information acquired during the identity authentication as first facial feature information of the user.

The sending unit 630 may be further configured to send the first facial feature information of the user to the server to enable the server to send the dynamic face authentication prompt information upon verifying that the first facial feature information matches second facial feature information of the user that is stored.

Optionally, the acquisition unit may be further configured to acquire facial feature information of the user when the user conducts registration, and use the facial feature information acquired during the registration as the second facial feature information of the user. The sending unit 630 may be further configured to send the second facial feature information to the server to allow the server to store a correspondence relationship between a user name of the user and the second facial feature.

Optionally, the acquisition unit may include a face tracking subunit configured to track the face of the user when the face of the user is detected; an image acquisition subunit configured to acquire a face image according to a preset time interval during face tracking; a

condition determination subunit configured to determine whether the face image meets a preset feature extraction condition; and a feature extraction subunit configured to extract facial feature information of the user from the face image in an event that the feature extraction condition is met.

The condition determination subunit may further include:

a resolution determination module configured to determine whether a resolution of the face image meets a preset resolution threshold;

a gesture information extraction module configured to extract head gesture information from the face image if the resolution threshold is met, the head gesture information including at least one of the following angles: a head lowering/raising angle, a face turning angle, or a head leaning angle;

an angle determination module configured to determine whether each angle included in the head gesture information falls within a respective preset angle range; and

a judgment determination module configured to determine that the face image meets the feature extraction condition if each angle falls within the respective preset angle range.

The feature extraction subunit may be specifically configured to extract a facial feature vector value from the face image as the facial feature information of the user using a preset feature extraction algorithm, wherein the preset feature extraction algorithm may include a Linear Back Projection (LBP) feature extraction algorithm, or a Gabor feature extraction algorithm in windowed Fourier transform.

FIG. 7 shows a block diagram of another embodiment of an identity authentication apparatus according to the present application. The identity authentication apparatus may be applied on a server. The apparatus includes a sending unit 710, a receiving unit 720, and a determination unit 730.

The sending unit 710 is configured to send dynamic face authentication prompt information to a terminal during identity authentication of a user.

The receiving unit 720 is configured to receive gesture recognition information sent by the terminal, the gesture recognition information being gesture recognition information obtained by the terminal through recognizing a facial gesture that is presented by the user according to the dynamic face authentication prompt information.

The determination unit 730 is configured to determine that the identity authentication of the user is successful in response to verifying that the gesture recognition information is consistent with the dynamic face authentication prompt information.

In an optional implementation, the receiving unit 720 may be further configured to receive first facial feature information of the user sent by the terminal.

The apparatus may further include (not shown in FIG. 7) a verification unit configured to verify whether the first facial feature information matches second facial feature information of the user that is stored.

The sending unit 710 may be specifically configured to send the dynamic face authentication prompt information to the terminal in response to a match therebetween.

Optionally, the receiving unit 720 may be further configured to receive the second facial feature information of the user sent by the terminal when the user conducts a registration. The apparatus may further include (not shown in FIG. 7) a storage unit configured to store a correspondence relationship between a user name of the user and the second facial feature information.

Optionally, the verification unit may include a feature searching subunit configured to search for the correspondence relationship based on the user name of the user to obtain the

second facial feature information corresponding to the user name; a feature comparison subunit configured to compare the first facial feature information and the second facial feature information in a preset comparison manner; and a matching determination subunit configured to determine that the first facial feature information matches the second facial feature information if a feature comparison value falls within a preset similarity range. The preset comparison manner used by the feature comparison subunit may include a method of Euclidean distance comparison, or a method of cosine distance comparison.

Details of processes of implementations of functions and effects of the various units in the foregoing apparatuses may be referenced to the processes of implementations of the corresponding steps in the foregoing methods, and are not repeatedly described herein.

Since the apparatus embodiments basically correspond to the method embodiments, related parts may be referenced to respective parts of the description of the method embodiments. The apparatus embodiments described above are merely exemplary. The units that are described as individual components may or may not be physically separate. A component displayed as a unit may or may not be a physical unit, i.e., may be located at a single place, or distributed among multiple network units. Some or all of the modules may be selected according to a real requirement to achieve the objective of the solutions of the present application. One of ordinary skill in the art can understand and implement the present application without making any creative effort.

As can be seen from the foregoing embodiments, a highly secure authentication can be performed on an identity of a user through dynamic face authentication during identity authentication of the user. As compared with existing authentication methods using an authentication password, authentication information will not be easily stolen by a malicious third party, thus improving the reliability of authentication. Moreover, a user can be

recognized as a live user through the dynamic face authentication, thereby further improving the accuracy of identity authentication and reducing potential security risks during authentication.

One skilled in the art can easily come up with other implementation solutions of the present application after considering the specification and practicing the invention disclosed herein. The present application is intended to cover any variations, usages, or adaptive changes of the present application. These variations, usages or adaptive changes follow general principles of the present application and include common knowledge or conventional technical measures in the present technical field that are not disclosed in the present application. The specification and embodiments are merely considered as exemplary, and the real scope and spirit of the present application are specified by the claims herein.

It should be noted that the present application is not limited to the precise structures that have been described above and illustrated in the accompanying drawings. Various modifications and changes can be made to the present application without departing from the scope thereof. The scope of the present application is only limited by the appended claims.

Claims

1. An identity authentication method, wherein the method comprises:

acquiring facial feature information of a user, the acquiring the facial feature information of the user comprising:

tracking (302) a face of the user upon detecting the face of the user;

acquiring (303) a face image according to a preset time interval when tracking the face;

determining (304) whether the face image meets a preset feature extraction condition; and

extracting (305) facial feature information of the user from the face image in response to the feature extraction condition being met;

using the facial feature information as first facial feature information of the user;

sending (308) the first facial feature information of the user to the server to allow the server to send the dynamic face authentication prompt information in response to verifying that the first facial feature information matches second facial feature information of the user that is stored;

receiving (201) the dynamic face authentication prompt information sent by a server during identity authentication of a user;

obtaining (202) gesture recognition information of the dynamic face authentication prompt information by recognizing a facial gesture presented by the user; and

sending (203) the gesture recognition information to the server to enable the server to confirm that the identity authentication is successful for the user upon verifying that the gesture recognition information is consistent with the dynamic face authentication prompt information.

2. The method of any preceding claim, wherein the method further comprises:

acquiring (303) facial feature information of the user when the user conducts registration, and using the facial feature information acquired during the registration as the second facial feature information of the user; and

sending (308) the second facial feature information to the server to enable the server to store (309) a correspondence relationship between a user name of the user and the second facial feature information.

3. The method of claim 1 or claim 2, wherein determining whether the face image meets the preset feature extraction condition comprises:

determining (304) whether a resolution of the face image meets a preset resolution threshold;

extracting (305) head gesture information from the face image if the resolution threshold is met, the head gesture information comprising at least one of the following angles: a head lowering/raising angle, a face turning angle, or a head leaning angle;

determining (306) whether each angle included in the head gesture information falls within a respective preset angle range; and

determining that the face image meets the feature extraction condition if each angle falls within the respective preset angle range.

4. The method of any preceding claim, wherein obtaining (202) the gesture recognition information of the dynamic face authentication prompt information by recognizing the facial gesture presented by the user, comprises:

obtaining (202) face tracking information by tracking a face of the user when the user presents a facial gesture according to the dynamic face authentication prompt information; and

analyzing the face tracking information to obtain the gesture recognition information of the user.

5. The method of claim 4, wherein analyzing the face tracking information to obtain the gesture recognition information of the user comprises:

when the face tracking information is facial key point position information, obtaining expression gesture recognition information of the user by analyzing the facial key point position information; or

when the face tracking information is head gesture information, obtaining head turning recognition information of the user by analyzing the head gesture information.

6. The method of any one of claims 1-5, wherein the dynamic face authentication prompt information comprises at least one type of the following information: expression action prompt information or voice read prompt information.

7. The method of claim 6, wherein the dynamic face authentication prompt information comprises the voice read prompt information, and obtaining (202) the gesture recognition information comprises:

obtaining mouth shapes and audio information of the user; and

recognizing one or more mouth shapes of the user when reading the voice read prompt information and obtaining voice information of the user from the audio information through voice recognition, wherein recognizing the one or more mouth shapes and obtaining the voice information enables the server to determine whether the voice information is consistent with the voice read prompt information when verifying the gesture recognition information, and the identity authentication is determined to be successful for the user upon verifying that the voice information is consistent with the voice read prompt

information and the gesture recognition information is consistent with the dynamic face authentication prompt information.

8. An identity authentication apparatus, wherein the apparatus comprises:

an acquisition unit configured to acquire (303) facial feature information of a user, and use the facial feature information acquired during the identity authentication as first facial feature information of the user, the acquisition unit comprising:

a face tracking subunit configured to track (302) a face of the user when the face of the user is detected;

an image acquisition subunit configured to acquire (303) a face image according to a preset time interval when the face is tracked;

a condition determination subunit configured to determine (304) whether the face image meets a preset feature extraction condition; and

a feature extraction subunit configured to extract (305) facial feature information of the user from the face image when the feature extraction condition is met;

a receiving unit (610) configured to receive (201) dynamic face authentication prompt information sent by a server during identity authentication of the user;

a recognition unit (620) configured to obtain (202) gesture recognition information of the dynamic face authentication prompt information by recognizing a facial gesture presented by the user; and

a sending unit (630), configured to:

send (308) the first facial feature information of the user to the server to allow the server to send the dynamic face authentication prompt information in response to verifying that the first facial feature information matches second facial feature information of the user that is stored, and

send (203) the gesture recognition information to the server to enable the server to confirm that the identity authentication of the user is successful upon verifying that the gesture recognition information is consistent with the dynamic face authentication prompt information.

9. The apparatus of claim 8, wherein the recognition unit (620) comprises:

a face information obtaining subunit configured to obtain face tracking information by tracking a face of the user when the user presents a facial gesture according to the dynamic face authentication prompt information; and

a face information analysis subunit configured to analyze the face tracking information to obtain the gesture recognition information of the user.

10. The apparatus of claim 9, wherein the face information analysis subunit is specifically configured to:

obtain expression gesture recognition information of the user by analyzing facial key point position information when the face tracking information is the facial key point position information; or

obtain head turning recognition information of the user by analyzing head gesture information when the face tracking information is the head gesture information.

11. The apparatus of any one of claims 8 to 10, wherein:

the acquisition unit is further configured to acquire facial feature information of the user during user registration, and use the facial feature information acquired during the registration as the second facial feature information of the user; and

the sending unit (630) is further configured to send (308) the second facial feature information to the server to allow the server to store (309) a correspondence relationship between a user name of the user and the second facial feature information.

12. The apparatus of any one of claims 8 to 11, wherein the condition determination subunit comprises:

a resolution determination module configured to determine whether a resolution of the face image meets a preset resolution threshold;

a gesture information extraction module configured to extract head gesture information from the face image if the resolution threshold is met, the head gesture information comprising at least one of the following angles: a head lowering/raising angle, a face turning angle, or a head leaning angle;

an angle determination module configured to determine whether each angle comprised in the head gesture information falls within a respective preset angle range; and

a judgment determination module configured to determine that the face image meets the feature extraction condition if each angle falls within the respective preset angle range.

13. A terminal comprising:

one or more processors; and

memory configured to store instructions executable by the one or more processors, the one or more processors configured to:

acquire facial feature information of a user, acquiring the facial feature information of the user comprising:

tracking (302) a face of the user upon detecting the face of the user;

acquiring (303) a face image according to a preset time interval when tracking the face;

determining (304) whether the face image meets a preset feature extraction condition; and

extracting (305) the facial feature information of the user from the face image in response to the feature extraction condition being met;

use the facial feature information as first facial feature information of the user;

send (308) the first facial feature information of the user to a server to allow the server to send dynamic face authentication prompt information in response to verifying that the first facial feature information matches second facial feature information of the user that is stored;

receive (201) the dynamic face authentication prompt information sent by a server during identity authentication of a user;

obtain (202) gesture recognition information of the dynamic face authentication prompt information by recognizing a facial gesture presented by the user; and

send (203) the gesture recognition information to the server to enable the server to confirm that the user passes the identity authentication upon verifying that the gesture recognition information is consistent with the dynamic face authentication prompt information.

14. The terminal of claim 13, wherein determining whether the face image meets the preset feature extraction condition comprises:

determining whether a resolution of the face image meets a preset resolution threshold;

extracting head gesture information from the face image if the resolution threshold is met, the head gesture information comprising at least one of a head lowering/raising angle, a face turning angle, or a head leaning angle;

determining whether each angle included in the head gesture information falls within a respective preset angle range; and

determining that the face image meets the feature extraction condition when each angle falls within the respective preset angle range.

15. The terminal of claim 13 or claim 14, wherein the dynamic face authentication prompt information comprises voice read prompt information, and obtaining the gesture recognition information comprises:

obtaining mouth shapes and audio information of the user; and

recognizing one or more mouth shapes of the user when reading the voice read prompt information and obtaining voice information of the user from the audio information through voice recognition, wherein recognizing the one or more mouth shapes and obtaining the voice information enables the server to determine whether the voice information is consistent with the voice read prompt information when verifying the gesture recognition information, and the identity authentication is determined to be successful for the user upon verifying that the voice information is consistent with the voice read prompt information and the gesture recognition information is consistent with the dynamic face authentication prompt information.