

AUTHENTICATION METHOD AND DEVICE, AND METHOD AND DEVICE FOR GENERATING INFORMATION FOR AUTHENTICATION

TECHNICAL FIELD

5 **[0001]** The present application relates to the field of information security technologies, and in particular, to an authentication method and device, and a method and a device for generating information for authentication.

BACKGROUND

10 **[0002]** With the rapid development of information technologies, users pay more attention to information security. Authentication is a common method used to ensure information security.

15 **[0003]** For example, a terminal device of a first user performs authentication. The first user can predetermine standard information (e.g., a password) for authentication. After the standard information is set, the terminal device can perform authentication on any user (referred to as a second user) performing a specific operation on the terminal device based on the standard information. If the second user can correctly enter the standard information, the terminal device can authenticate the second user as the first user. Otherwise, the terminal device can determine that the second user is not the first user but an attacker, and therefore, can prevent the second user from performing the specific operation. As such, information security of the first user on the terminal device can be improved. The specific operation can be a screen unlock operation, a login operation, a personal information modification operation, a payment operation, etc.

25 **[0004]** In the existing technology, the standard information can be a gesture password, and authentication can be performed based on the gesture password. Specifically, there are nine key node areas in a gesture password input interface provided by an operating system or an application of the terminal device, and the nine key node areas are distributed in the form of a nine-box grid, as shown in the gesture

password input interface in FIG. 1. The first user can set a two-dimensional track that connects at least two key node areas as the gesture password. After the gesture password is set, when the terminal device performs authentication on the second user, the second user can be authenticated only when the second user connects key node areas in the gesture password input interface to reproduce a gesture corresponding to the gesture password.

[0005] However, gesture password input interfaces in the existing technology are undiversified, and attackers are usually familiar with the gesture password input interface. Therefore, the difficulty of the attacker in peeping at and memorizing the gesture password entered by the first user is reduced, and/or the difficulty of the attacker in cracking the gesture password set by the first user through exhaustive attack is reduced, causing relatively low authentication reliability.

SUMMARY

[0006] Implementations of the present application provide an authentication method and device, to alleviate a problem of relatively low authentication reliability caused by undiversified gesture password input interfaces in the existing technology.

[0007] The implementations of the present application provide a method and a device for generating information for authentication.

[0008] The following technical solutions are used in the implementations of the present application:

[0009] The authentication method provided in the implementations of the present application includes the following: displaying a picture pre-specified by a first user; detecting an interactive operation of a second user for the picture; generating interactive operation information of the second user based on the detected interactive operation of the second user; and performing authentication to determine whether the second user is the first user by matching the interactive operation information of the second user and standard information, where the standard information is generated based on an interactive operation of the first user for the picture.

[0010] The authentication device provided in the implementations of the present application includes a display module, configured to display a picture pre-specified by a first user; a detection module, configured to detect an interactive operation of a second user for the picture; a generation module, configured to generate interactive

operation information of the second user based on the detected interactive operation of the second user; and an authentication module, configured to perform authentication to determine whether the second user is the first user by matching the interactive operation information of the second user and standard information, where the standard information is generated based on an interactive operation of the first user for the picture.

[0011] The method for generating information for authentication provided in the implementations of the present application includes the following: obtaining a picture specified by a first user; displaying the picture, and determining one or more feature areas on the picture; detecting an interactive operation of the first user for the one or more feature areas; and generating standard information based on the detected interactive operation of the first user so as to perform authentication to determine whether a second user is the first user.

[0012] The device for generating information for authentication provided in the implementations of the present application includes an acquisition module, configured to obtain a picture specified by a first user; a display and determining module, configured to display the picture, and determine one or more feature areas on the picture; a detection module, configured to detect an interactive operation of the first user for the one or more feature areas; and a generation module, configured to generate standard information based on the detected interactive operation of the first user, so as to perform authentication to determine whether a second user is the first user.

[0013] The at least one technical solutions used in the implementations of the present application can achieve the following beneficial effects: The picture specified by the first user can be used as a gesture password input interface customized by the first user, and the interactive operation can include a gesture, to diversify gesture password input interfaces. Feature area locations of gesture password input interfaces corresponding to different pictures are usually different, and a feature area location of the gesture password input interface corresponding to the picture specified by the first user is also different from a feature area location of a gesture password input interface in the existing technology. Therefore, an attacker may not be familiar with the gesture password input interface corresponding to the picture. As such, the difficulty of the attacker in peeping at and memorizing the gesture password entered by the first user can be increased, and/or the difficulty of the attacker in cracking the gesture password

set by the first user through exhaustive attack can be increased, thereby improving authentication reliability. Therefore, the present application can partly or wholly alleviate the problem in the existing technology.

BRIEF DESCRIPTION OF DRAWINGS

- 5 **[0014]** The accompanying drawings here are used to provide further understanding of the present application, and constitute a part of the present application. Example implementations of the present application and descriptions of the implementations are used to explain the present application, and do not constitute an improper limitation to the present application. In the accompanying drawings:
- 10 **[0015]** FIG. 1 is a schematic diagram illustrating a gesture password input interface in the existing technology;
- [0016]** FIG. 2 is a schematic flowchart illustrating an authentication method, according to an implementation of the present application;
- [0017]** FIG. 3 is a schematic flowchart of generating standard information in FIG.
- 15 2, according to an implementation of the present application;
- [0018]** FIG. 4 illustrates two examples of a specific picture, according to an implementation of the present application;
- [0019]** FIG. 5 is a schematic diagram of a feature area determined and marked on a specific picture, according to an implementation of the present application;
- 20 **[0020]** FIG. 6 is a schematic diagram of a specific picture when a feature area is marked or unmarked, according to an implementation of the present application;
- [0021]** FIG. 7 is a schematic flowchart illustrating a method for generating information for authentication, according to an implementation of the present application;
- 25 **[0022]** FIG. 8 is a detailed schematic flowchart of generating standard information in actual application scenarios, according to an implementation of the present application;
- [0023]** FIG. 9 is a schematic diagram of a standard information input interface in another existing technology;
- 30 **[0024]** FIG. 10 is a schematic structural diagram illustrating an authentication device, according to an implementation of the present application; and
- [0025]** FIG. 11 is a schematic structural diagram illustrating a device for

generating information for authentication, according to an implementation of the present application.

DESCRIPTION OF IMPLEMENTATIONS

[0026] To make the objectives, technical solutions, and advantages of the present application clearer, the following clearly and completely describes the technical solutions of the present application with reference to the specific implementations and the corresponding accompanying drawings of the present application. Apparently, the described implementations are some rather than all of the implementations of the present application. All other implementations obtained by a person of ordinary skill in the art based on the implementations of the present application without creative efforts shall fall within the protection scope of the present application.

[0027] The solutions of the present application can be used for authentication, for example, can be used to perform authentication on a second user (that is, a user to be authenticated) when the second user performs a specific operation. The specific operation can be a screen unlock operation, a login operation, a personal information modification operation, a payment operation, etc. The solutions of the present application can partly or wholly alleviate the problem in the existing technology, and the following describes the solutions of the present application.

[0028] FIG. 2 is a schematic flowchart illustrating an authentication method, according to an implementation of the present application. The procedure can be performed by an authentication-related device. The device includes but is not limited to a mobile phone, a tablet, a smart watch, a vehicle mobile system, a personal computer, a large or medium-sized computer, a computer cluster, etc. The execution body does not constitute a limitation to the present application.

[0029] The procedure in FIG. 2 can include the following steps.

[0030] S201. Display a picture pre-specified by a first user.

[0031] For ease of description, the picture pre-specified by the first user in step S201 can be referred to as a specific picture below.

[0032] In this implementation of the present application, before the procedure in FIG. 2 is performed, standard information used for authentication can be generated in advance based on operation of the first user. In the procedure in FIG. 2, authentication is performed on a second user based on the standard information. In practice, the

second user can be the first user, or the second user can be a user other than the first user, for example, an attacker. It can be determined whether the second user is the first user through authentication in the procedure in FIG. 2.

[0033] In this implementation of the present application, the standard information can be generated based on the specific picture, and the specific picture is specified by the first user. For example, the first user can specify a picture prestored locally or on a cloud as the specific picture, or can specify a new picture obtained in a specific way as the specific picture. For example, an execution body with a camera can take a picture and specify the picture as the specific picture.

[0034] S202. Detect an interactive operation of a second user for the picture.

[0035] In this implementation of the present application, in step S202, an interactive operation of the second user for any area on the picture can be detected, or an interactive operation of the second user for only one or more feature areas on the picture can be detected.

[0036] S203. Generate interactive operation information of the second user based on the detected interactive operation of the second user.

[0037] In this implementation of the present application, the interactive operation can be one or more operations such as tapping, sliding, and pressing, and the interactive operation information can reflect interactive operation content corresponding to the interactive operation information.

[0038] It is worthwhile to note that the listed operations are merely examples of interactive operations, and the interactive operation can be operations other than these operations. Operations such as tapping, sliding, and pressing can be further divided so that the interactive operation content is described by using more specific features (the interactive operation content is more specific). For example, the tapping operation can be further divided based on features such as tapping force, tapping time, number of taps, and tapping frequency, the sliding operation can be further divided based on features such as sliding track, sliding time, sliding force, and sliding distance, and the pressing operation can be further divided based on features such as pressing time and pressing force.

[0039] A level of specificity of the interactive operation content is not limited in the present application. Generally, when the interactive operation content is more specific, the corresponding interactive operation information generated can also be more specific, and authentication can also be performed more strictly based on the

interactive operation information. The level of specificity of the interactive operation content can be pre-specified as actually required.

[0040] For example, the interactive operation is the tapping operation. When the specified level of specificity is relatively low, only the number of taps can be detected,
5 but the tapping force or the tapping time is not detected. When the specified level of specificity is relatively high, the number of taps, the tapping force, the tapping time, etc. can be detected.

[0041] For another example, the interactive operation is the sliding operation. When the specified level of specificity is relatively low, only the sliding track can be
10 detected, but the sliding time or the sliding force is not detected. When the specified level of specificity is relatively high, the sliding track, the sliding time, the sliding force, etc. can be detected.

[0042] S204. Perform authentication to determine whether the second user is the first user by matching the interactive operation information of the second user and
15 standard information, where the standard information is generated based on an interactive operation of the first user for the picture.

[0043] In this implementation of the present application, as described above, after the standard information used for authentication is generated in advance, a picture (that is, the specific picture) for generating the standard information can be displayed
20 when authentication needs to be performed on the second user (corresponding to step S201). The second user can be authenticated only when the second user reproduces an interactive operation corresponding to the standard information for the specific picture displayed (corresponding to steps S202 to S204). The interactive operation corresponding to the standard information is the interactive operation of the first user
25 for the picture used to generate the standard information.

[0044] For example, the specific picture can be used as a gesture password input interface customized by the first user. In this case, an interactive operation of the first user for one or more feature areas on the specific picture can be considered as a gesture, and the specified standard information can be considered as a gesture
30 password. During authentication, the specific picture can be displayed, and the second user can be authenticated only when the second user performs an interactive operation for the one or more feature areas on the specific picture to reproduce the gesture of the first user.

[0045] In this implementation of the present application, it can be seen from the

previous descriptions that the interactive operation information of the second user can reflect interactive operation content of the second user for the specific picture, and the standard information can reflect interactive operation content of the first user for the specific picture. Therefore, it can be determined whether the second user has reproduced the operation of the first user by matching the interactive operation information of the second user and the standard information, to further determine whether the second user is the first user through authentication.

[0046] It is worthwhile to note that a specific detection method used to detect the interactive operation of the second user is usually the same as or similar to a specific detection method used to detect the interactive operation of the first user during generation of the standard information (otherwise, it is inappropriate to match the interactive operation information of the second user and the standard information because comparability between the interactive operation information of the second user and the standard information may be relatively low). As such, the interactive operation information of the second user and the standard information can be matched, and the method for performing authentication based on interactive operation information matching can be more reliable in the present application.

[0047] based on the previously described method, the picture specified by the first user can be used as the gesture password input interface customized by the first user, and the interactive operation can include a gesture, to diversify gesture password input interfaces. Feature area locations of gesture password input interfaces corresponding to different pictures are usually different, and a feature area location of the gesture password input interface corresponding to the picture specified by the first user is also different from a feature area location of a gesture password input interface in the existing technology. Therefore, an attacker may not be familiar with the gesture password input interface corresponding to the picture. As such, the difficulty of the attacker in peeping at and memorizing the gesture password entered by the first user can be increased, and/or the difficulty of the attacker in cracking the gesture password set by the first user through exhaustive attack can be increased, thereby improving authentication reliability. Therefore, the present application can partly or wholly alleviate the problem in the existing technology.

[0048] In addition, the method has more advantages compared with the existing technology. Specifically, a gesture in the existing technology corresponds to a relatively small quantity of operation types, a level of specificity is also relatively low,

and only a sliding operation is usually included. Corresponding gesture information generated usually describes only a sliding track, but does not describe sliding time, sliding force, or other feature information. In addition to the gesture (the sliding operation) in the existing technology, the interactive operation in the present application can include more operation types (e.g., a tapping operation and a pressing operation). For the operation types included, a level of specificity can be customized for interactive operation content generated through these operations, so that interactive operation information generated can be more specific (compared with the gesture information in the existing technology), thereby making authentication stricter and improving information security of the first user.

[0049] In addition, based on the previously described method, a user can choose not to use the specific gesture password input interface in the existing technology, but freely select a picture that the user likes so as to generate a corresponding gesture password input interface. Thus, the gesture password input interface can be better customized and user experience can be improved.

[0050] It is worthwhile to note that the steps in the procedure in FIG. 2 can be performed by one device, or can be performed by different devices. For example, step 201 can be performed by device 1, and steps 202 to 204 can be performed by device 2; or steps 201 to 203 can be performed by device 1, and step 204 can be performed by device 2.

[0051] Based on the previously described method, this implementation of the present application further provides some specific implementation solutions of the authentication method and extension solutions, which are described below.

[0052] In this implementation of the present application, as mentioned above, the standard information in FIG. 2 can be generated based on the interactive operation of the first user for the picture. For ease of understanding, the following describes a procedure of generating the standard information in FIG. 2, as shown in FIG. 3.

[0053] FIG. 3 is a schematic flowchart of generating the standard information in FIG. 2, according to an implementation of the present application. An execution body of the procedure in FIG. 3 and the execution body of the procedure in FIG. 2 can be the same device, or can be different devices.

[0054] The procedure in FIG. 3 can include the following steps.

[0055] S301. Obtain a picture (that is, a specific picture) specified by a first user.

[0056] In this implementation of the present application, related information such

as content and format of the specific picture is not limited. Two examples of the specific picture are provided in this implementation of the present application, as shown in FIG. 4.

[0057] FIG. 4 illustrates two examples of a specific picture, according to the present application, which are respectively the picture of a dog on the left side in FIG. 4 and the picture of a cat on the right side in FIG. 4. For ease of description, the following implementation is also described based on the specific picture examples in FIG. 4.

[0058] S302. Display the picture, and determine one or more feature areas on the picture.

[0059] In this implementation of the present application, feature detection can be performed on the specific picture based on a specific picture feature area detection algorithm, to determine the one or more feature areas on the specific picture. The feature area can be specified by the execution body or specified by the first user. Based on the method for determining the feature area, user operations and intervention are reduced, and automation degree of the solutions of the present application is improved.

[0060] The picture feature area detection algorithm is not limited in the present application, and some example algorithms are listed here. The picture feature area detection algorithm can be scale-invariant feature transform (SIFT) algorithm, speeded up robust features (SURF) algorithm, features from accelerated segment test (FAST) algorithm, oriented FAST and rotated BRIEF (ORB) algorithm, Harris algorithm, binary robust invariant scalable keypoints (BRISK) algorithm, etc. Because different picture feature area detection algorithms can focus on different features, feature areas that can be detected by using different picture feature area detection algorithms can also be different. For example, a circular area on a specific picture can usually be detected by using the SURF algorithm and used as a feature area; and an angular area on a specific picture can usually be detected by using the Harris algorithm and used as a feature area. During implementation of the solutions of the present application, one or more picture feature area detection algorithms can be selected as the specific picture feature area detection algorithm as actually required.

[0061] It is worthwhile to note that the number of feature areas that can be determined can vary for different specific pictures. When there are excessive feature areas (for example, a dozen or dozens of feature areas are determined on a specific

picture), subsequent operations cannot be performed easily. When there are few feature areas (for example, only one or two feature areas are determined on a specific picture), authentication cannot be performed strictly as expected. To alleviate the problem, the number of feature areas determined or the number of feature areas used for authentication can be limited. For example, the number of feature areas determined by the first user on each specific picture can be limited to 9 or another value. If the limited number is exceeded, some feature areas can be removed, or if the limited number is not reached, some feature areas can be added. As such, the number of feature areas can be appropriate.

[0062] In this implementation of the present application, the feature area can also be determined not based on the specific picture feature area detection algorithm, but the first user can directly specify one or more areas on the specific picture as the feature area. The method for determining the feature area has the following advantages: The first user has relatively strong control over the feature area, and because the feature area is specified by the first user, the first user can memorize the feature area more easily.

[0063] It can be seen from the previous analysis on the method for determining the feature area that, in this implementation of the present application, the determining one or more feature areas on the picture in step S302 can include the following: performing feature detection on the picture, and determining the one or more feature areas on the specific picture through feature detection; and/or determining one or more areas specified by the first user on the specific picture, and using the one or more areas as the feature area.

[0064] In this implementation of the present application, after the feature area is determined, the feature area determined can also be marked on the specific picture displayed, so that the first user can know the feature area determined and can perform an interactive operation for the feature area. The marking can be performed in the form of a text and/or a graphic and/or a color, etc., and the marking can be used to indicate that an area corresponding to the marking is the feature area.

[0065] This implementation of the present application provides a schematic diagram of a feature area determined and marked on a specific picture, as shown in FIG. 5. The specific picture in FIG. 4 is used as an example.

[0066] In FIG. 5, each feature area determined on the specific picture is marked by using a circular graphic. Five feature areas are marked on the specific picture on

the left side in FIG. 5, and three feature areas are marked on the specific picture on the right side in FIG. 5.

[0067] S303. Detect an interactive operation of the first user for the one or more feature areas.

5 **[0068]** S304. Generate standard information based on the detected interactive operation of the first user.

[0069] In this implementation of the present application, after the standard information is generated, the authentication procedure can be triggered when a predetermined condition is satisfied. In practice, to adjust the strictness of authentication, before the authentication (e.g., before step S201 is performed), setting can be performed for the one or more feature areas. The setting is used to determine whether to mark the one or more feature areas on the displayed picture pre-specified by the first user.

15 **[0070]** If, through setting, the feature area is marked on the specific picture displayed during authentication, the second user can directly know the feature area on the specific picture due to the marking, which helps the second user reproduce the interactive operation of the first user for the feature area. Therefore, the strictness of authentication is relatively low.

20 **[0071]** If through setting, the feature area is unmarked on the specific picture displayed during authentication, the second user cannot directly know the feature area on the specific picture. If the second user is not the first user, the second user can hardly determine the feature area on the specific picture, and therefore, can hardly reproduce the interactive operation for the feature area. As such, the strictness of authentication is relatively high, thereby improving information security of the first user.

[0072] This implementation of the present application provides a schematic diagram of a specific picture when a feature area is marked or unmarked, as shown in FIG. 6. The specific picture on the left side in FIG. 4 is used as an example.

30 **[0073]** In FIG. 6, the left side in FIG. 6 is a schematic diagram of a specific picture with a marked feature area, and the right side in FIG. 6 is a schematic diagram of a specific picture with an unmarked feature area.

[0074] In this implementation of the present application, as mentioned above, interactive operation information can reflect corresponding interactive operation content, and the reflection can be implemented in a plurality of specific methods. Two

specific methods are listed as examples below.

[0075] Specific method 1: An operation order for feature areas on a specific picture can be a part of interactive operation content. Interactive operation information can reflect only the part of corresponding interactive operation content.

5 **[0076]** In this case, for ease of representing the operation order, after the one or more feature areas are determined on the specific picture, corresponding identification information can be further generated for each feature area. The identification information can be used to uniquely determine a feature area corresponding to the identification information on the specific picture. For example, the identification
10 information can be coordinate information of the feature area corresponding to the identification information, or can be a character or a character string such as a number or a letter uniquely corresponding to the coordinate information of the feature area corresponding to the identification information.

[0077] During generation of the standard information, the generating standard
15 information based on the detected interactive operation of the first user in step S304 can include the following: determining an operation order of the first user for the one or more feature areas based on the detected interactive operation of the first user; and generating a feature area identification information sequence used to indicate the operation order based on the operation order and identification information
20 corresponding to the one or more feature areas, and using the feature area identification information sequence as the standard information.

[0078] For example, assume that three feature areas are determined on a specific picture, and identification information corresponding to the three feature areas is generated: respectively numbers "1", "2", and "3". Assume that interactive operations
25 of the user for the three feature areas are sequentially performing a tapping operation for the three feature areas. In this case, an operation order of the first user for the three feature areas is the first feature area, the second feature area, and the third feature area. The operation sequence is represented by using the identification information of the feature areas, and therefore, a feature area identification information sequence "1, 2,
30 3" or "123" is generated and used as the standard information. It is worthwhile to note that "1, 2, 3" and "123" in this example are examples of the feature area identification information sequence, and do not constitute a limitation. In practice, the feature area identification information sequence can be represented in a form other than the digital sequence, provided that the feature area identification information sequence can

indicate the operation order of the first user for the feature areas.

[0079] Correspondingly, during authentication, specific method 1 can also be used to generate interactive operation information of the second user. The generating interactive operation information of the second user based on the detected interactive operation of the second user in step 203 can include the following: determining an operation order of the second user for the one or more feature areas based on the detected interactive operation of the second user, when it is determined that the interactive operation of the second user includes an interactive operation of the second user for the one or more feature areas; and generating a feature area identification information sequence used to indicate the operation order based on the operation order and the identification information corresponding to the one or more feature areas, and using the feature area identification information sequence as the interactive operation information of the second user.

[0080] Specific method 2: In addition to the operation order, the interactive operation information can reflect more specific interactive operation content. For example, when the interactive operation is a sliding operation, not only an operation order (that is, a sliding track) can be reflected, but also a sliding force can be reflected.

[0081] During generation of the standard information, the generating standard information based on the detected interactive operation of the first user in step S304 can include the following: determining an operation order of the first user for the one or more feature areas and an operation feature representation value of the one or more feature areas based on the detected interactive operation of the first user, where the operation feature representation value is used to represent an operation feature when the first user performs the interactive operation for the feature area corresponding to the operation feature representation value; and generating a feature area identification information and operation feature representation value sequence used to indicate the operation order and the operation feature based on the operation order, identification information corresponding to the one or more feature areas, and the operation feature representation value of the one or more feature areas, and using the feature area identification information and operation feature representation value sequence as the standard information.

[0082] For example, three feature areas are determined on a specific picture, and identification information corresponding to the three feature areas is generated:

respectively numbers "1", "2", and "3". Assume that interactive operations of the user for the three feature areas are performing sliding from the first feature area to the second feature area, and then performing sliding from the second feature area to the third feature area. In this case, an operation order of the first user for the three feature areas is the first feature area, the second feature area, and the third feature area. Further, assume that an operation feature is a sliding force, and the sliding force is classified into "A" and "B" by force. In this case, an operation feature representation value can be "A" or "B".

[0083] Assume that a sliding force of the first user for performing sliding from the first feature area to the second feature area is "A", and a sliding force of the first user for performing sliding from the second feature area to the third feature area is "B". In this case, a feature area identification information and operation feature representation value sequence can be generated and used as the standard information: "1, A, 2, B, 3" or "1A2B3". It is worthwhile to note that "1, A, 2, B, 3" and "1A2B3" in this example are examples of the feature area identification information and operation feature representation value sequence, and do not constitute a limitation. In practice, the feature area identification information and operation feature representation value sequence can be represented in a form other than the digital letter sequence, provided that the feature area identification information and operation feature representation value sequence can indicate the operation order of the first user for the feature areas and the operation feature.

[0084] Correspondingly, during authentication, specific method 2 can also be used to generate interactive operation information of the second user. Details are omitted here for simplicity.

[0085] In this implementation of the present application, during generation of the standard information, to prevent the first user from performing a misoperation, the first user can usually reconfirm the operation (referred to as standard information double confirmation) on the generated standard information. Specifically, standard information can be re-generated and compared with the standard information generated before. If the comparison result is that they are the same, it is determined that the standard information generated can be used for authentication.

[0086] Based on the previous descriptions of generating the standard information, an implementation of the present application provides a method for generating information for authentication. Standard information can be generated by performing

the method for generating information, and a procedure of the method for generating information is shown in FIG. 7.

[0087] The procedure in FIG. 7 can include the following steps.

[0088] S701. Obtain a picture specified by a first user.

5 [0089] S702. Display the picture, and determine one or more feature areas on the picture.

[0090] S703. Detect an interactive operation of the first user for the one or more feature areas.

[0091] S704. Generate standard information based on the detected interactive
10 operation of the first user so as to perform authentication to determine whether a second user is the first user.

[0092] In this implementation of the present application, the determining one or more feature areas on the picture in step S702 can include the following: performing feature detection on the picture, and determining the one or more feature areas on the
15 specific picture through feature detection; and/or determining one or more areas specified by the first user on the specific picture, and using the one or more areas as the feature area.

[0093] Further, based on the procedure in FIG. 7 and an extension solution related to the previously described generation of standard information, an implementation of
20 the present application further provides a detailed schematic flowchart of generating standard information in actual application scenarios, as shown in FIG. 8. In the actual application scenarios, an interactive operation is a tapping operation.

[0094] The procedure in FIG. 8 can include the following steps.

[0095] S801. Receive a customized picture uploaded by a first user.

25 [0096] S802. Determine a picture feature detection algorithm specified by the first user, and determine a plurality of feature areas on the received picture based on the picture feature detection algorithm.

[0097] S803. Display the picture, mark the feature area, and generate corresponding identification information for the feature area.

30 [0098] S804. Detect a tapping operation of the first user for the feature area.

[0099] S805. Generate a feature area identification information sequence used to indicate a detected tapping order of the first user for the feature area, based on the identification information of the feature area and the tapping order, and use the feature area identification information sequence as standard information.

[0100] S806. Receive a double confirmation of the first user for the standard information.

[0101] S807. Determine whether to mark the feature area on the displayed picture during standard information authentication based on an indication of the first user.

5 **[0102]** In this implementation of the present application, when standard information of the previous sequence form and interactive operation information of a second user are identical, it can usually be determined that the second user has reproduced the interactive operation of the first user. In this case, the performing authentication to determine whether the second user is the first user by matching the
10 interactive operation information of the second user and standard information in step 204 can include the following: determining whether the interactive operation information of the second user and the standard information are the same by matching the interactive operation information of the second user and the standard information; and if yes, authenticating the second user as the first user; otherwise, not
15 authenticating the second user as the first user.

[0103] In this implementation of the present application, in practice, the second user can also be authenticated as the first user without a requirement that the standard information and the interactive operation information of the second user are the same. Instead, it can be determined whether an interactive operation of the second user and
20 an interactive operation of the first user are the same or similar by matching the standard information and the interactive operation information of the second user, and then authentication is performed based on the determining result. In this case, the performing authentication to determine whether the second user is the first user by matching the interactive operation information of the second user and standard
25 information in step 204 can include the following: determining whether an interactive operation corresponding to the interactive operation information of the second user and an interactive operation corresponding to the standard information are the same, by matching the interactive operation information of the second user and the standard information; if yes, authenticating the second user as the first user; or determining
30 whether a similarity between an interactive operation corresponding to the interactive operation information of the second user and an interactive operation corresponding to the standard information is not less than a predetermined similarity threshold, by matching the interactive operation information of the second user and the standard information; if yes, authenticating the second user as the first user; otherwise, not

authenticating the second user as the first user.

[0104] In this implementation of the present application, the interactive operation for the picture can usually include a tapping operation for the one or more feature areas on the picture; and/or a sliding operation for performing sliding from one feature area to another when there are a plurality of feature areas on the picture. In addition, the interactive operation can further include a pressing operation for the one or more feature areas on the specific picture, etc.

[0105] In practice, in addition to the existing technology mentioned in the background, there is another commonly used existing technology for authentication. However, the other existing technology also has a problem similar to that in the existing technology mentioned in the background.

[0106] FIG. 9 is a schematic diagram of a password input interface in another existing technology. In this case, a password is a predetermined digital sequence, and a second user can be authenticated only when the second user taps digital areas in the password input interface to enter the password.

[0107] However, the password input interface in FIG. 9 is undiversified, and an attacker is usually familiar with such password input interface, which can cause relatively low authentication reliability.

[0108] To alleviate the previously described problem in the existing technology, based on the solutions of the present application, a first user can customize a password input interface, and a password can be the previously described standard information, so that the password input interface can be customized and diversified. Because an attacker may not be familiar with the password input interface customized by the first user, the difficulty of the attacker in peeping at and memorizing the password entered by the first user can be increased, and/or the difficulty of the attacker in cracking the password set by the first user through exhaustive attack can be increased, thereby improving authentication reliability. Therefore, the present application can also partly or wholly alleviate the other problem in the existing technology.

[0109] The authentication method and the method for generating information for authentication provided in the implementations of the present application are described above. Based on the same idea, the implementations of the present application further provide a corresponding authentication device and a corresponding device for generating information for authentication, as shown in FIG. 10 and FIG.

11.

[0110] FIG. 10 is a schematic structural diagram illustrating an authentication device, according to an implementation of the present application. The device includes a display module 1001, configured to display a picture pre-specified by a first user; a detection module 1002, configured to detect an interactive operation of a second user for the picture; a generation module 1003, configured to generate interactive operation information of the second user based on the detected interactive operation of the second user; and an authentication module 1004, configured to perform authentication to determine whether the second user is the first user by matching the interactive operation information of the second user and standard information, where the standard information is generated based on an interactive operation of the first user for the picture.

[0111] Optionally, the device further includes a standard information module 1005, configured to generate the standard information based on the interactive operation of the first user for the picture in the following way: obtaining the picture specified by the first user; displaying the picture, and determining one or more feature areas on the picture; detecting an interactive operation of the first user for the one or more feature areas; and generating the standard information based on the detected interactive operation of the first user.

[0112] Optionally, the standard information module 1005 is configured to perform feature detection on the picture, and determine the one or more feature areas on the specific picture through feature detection; and/or determine one or more areas specified by the first user on the specific picture, and use the one or more areas as the feature area.

[0113] Optionally, the standard information module 1005 is configured to perform setting for the one or more feature areas before the display module 1001 displays the picture pre-specified by the first user, where the setting is used to determine whether to mark the one or more feature areas on the displayed picture pre-specified by the first user.

[0114] Optionally, the standard information module 1005 is configured to generate corresponding identification information for each feature area after determining the one or more feature areas on the picture; determine an operation order of the first user for the one or more feature areas based on the detected interactive operation of the first user; and generate a feature area identification information

sequence used to indicate the operation order based on the operation order and identification information corresponding to the one or more feature areas, and use the feature area identification information sequence as the standard information; determine an operation order of the second user for the one or more feature areas
5 based on the detected interactive operation of the second user, when it is determined that the interactive operation of the second user includes an interactive operation of the second user for the one or more feature areas; and generate a feature area identification information sequence used to indicate the operation order based on the operation order and the identification information corresponding to the one or more
10 feature areas, and use the feature area identification information sequence as the interactive operation information of the second user.

[0115] Optionally, the authentication module 1004 is configured to determine whether the interactive operation information of the second user and the standard information are the same by matching the interactive operation information of the
15 second user and the standard information; and if yes, authenticate the second user as the first user.

[0116] Optionally, the authentication module 1004 is configured to determine whether an interactive operation corresponding to the interactive operation information of the second user and an interactive operation corresponding to the
20 standard information are the same by matching the interactive operation information of the second user and the standard information, and if yes, authenticate the second user as the first user; or determine whether a similarity between an interactive operation corresponding to the interactive operation information of the second user and an interactive operation corresponding to the standard information is not less than
25 a predetermined similarity threshold, by matching the interactive operation information of the second user and the standard information, and if yes, authenticate the second user as the first user.

[0117] Optionally, the interactive operation for the picture includes a tapping operation for the one or more feature areas on the picture; and/or a sliding operation
30 of performing sliding from one feature area to another when there are a plurality of feature areas on the picture.

[0118] The device in FIG. 10 can be located in an authentication-related device.

[0119] FIG. 11 is a schematic structural diagram illustrating a device for generating information for authentication, according to an implementation of the

present application. The device includes an acquisition module 1101, configured to obtain a picture specified by a first user; a display and determining module 1102, configured to display the picture, and determine one or more feature areas on the picture; a detection module 1103, configured to detect an interactive operation of the first user for the one or more feature areas; and a generation module 1104, configured to generate standard information based on the detected interactive operation of the first user, so as to perform authentication to determine whether a second user is the first user.

[0120] Optionally, the display and determining module 1102 is configured to perform feature detection on the picture, and determine the one or more feature areas on the specific picture through feature detection; and/or determine one or more areas specified by the first user on the specific picture, and use the one or more areas as the feature area.

[0121] The device in FIG. 11 can be located in an authentication-related device.

[0122] The devices provided in the present application are in a one-to-one mapping relationship with the methods provided in the present application. Therefore, the devices also have beneficial technical effects similar to those of the methods. Because the beneficial technical effects of the methods have been described in detail, beneficial technical effects of the devices are omitted here for simplicity.

[0123] A person skilled in the art should understand that the implementations of the present disclosure can be provided as a method, a system, or a computer program product. Therefore, the present disclosure can use a form of hardware only implementations, software only implementations, or implementations with a combination of software and hardware. Moreover, the present disclosure can use a form of a computer program product that is implemented on one or more computer-usable storage media (including but not limited to a magnetic disk storage, a CD-ROM, an optical memory, etc.) that include computer-usable program code.

[0124] The present disclosure is described with reference to the flowcharts and/or block diagrams of the method, the device (system), and the computer program product according to the implementations of the present disclosure. It should be understood that computer program instructions can be used to implement each process and/or each block in the flowcharts and/or the block diagrams and a combination of a process and/or a block in the flowcharts and/or the block diagrams. These computer program instructions can be provided for a general-purpose computer, a dedicated computer, an

embedded processor, or a processor of another programmable data processing device to generate a machine, so that the instructions executed by the computer or the processor of another programmable data processing device generate an apparatus for implementing a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0125] These computer program instructions can be stored in a computer readable memory that can instruct the computer or another programmable data processing device to work in a specific method, so that the instructions stored in the computer readable memory generate an artifact that includes an instruction apparatus. The instruction apparatus implements a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0126] These computer program instructions can be loaded onto the computer or another programmable data processing device, so that a series of operations and steps are performed on the computer or the another programmable device, thereby generating computer-implemented processing. Therefore, the instructions executed on the computer or another programmable device provide steps for implementing a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0127] In a typical configuration, a computing device includes one or more processors (CPU), an input/output interface, a network interface, and a memory.

[0128] The memory can include a non-persistent storage, a random access memory (RAM), a nonvolatile memory, and/or another form that are in a computer readable medium, for example, a read-only memory (ROM) or a flash memory (flash RAM). The memory is an example of the computer readable medium.

[0129] The computer readable medium includes persistent, non-persistent, movable, and unmovable media that can implement information storage by using any method or technology. Information can be a computer readable instruction, a data structure, a program module, or other data. A computer storage medium includes but is not limited to a phase-change random access memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), a random access memory (RAM) of another type, a read-only memory, an electrically erasable programmable read-only memory (EEPROM), a flash memory or another memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD), or another optical storage, a cassette, a cassette magnetic disk storage, or

another magnetic storage device or any other non-transmission medium. The computer storage medium can be configured to store information that can be accessed by the computing device. Based on the definition in the present specification, the computer readable medium does not include transitory computer-readable media
5 (transitory computer-readable media), for example, a modulated data signal and carrier.

[0130] It is worthwhile to further note that the term "include", "contain", or any other variant thereof is intended to cover a non-exclusive inclusion, so that a process, a method, an article, or a device that includes a list of elements not only includes
10 those elements but also includes other elements which are not expressly listed, or further includes elements inherent to such a process, method, article, or device. An element preceded by "includes a..." does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or device that includes the element.

[0131] A person skilled in the art should understand that the implementations of the present application can be provided as a method, a system, or a computer program product. Therefore, the present application can use a form of hardware only implementations, software only implementations, or implementations with a combination of software and hardware. Moreover, the present application can use a
15 form of a computer program product that is implemented on one or more computer-usable storage media (including but not limited to a magnetic disk storage, a CD-ROM, an optical memory, etc.) that include computer-usable program code.

[0132] The previous descriptions are merely implementations of the present application, and are not intended to limit the present application. For a person skilled
20 in the art, the present application can have various modifications and changes. Any modifications, equivalent substitutions, improvements, etc. made in the spirit and principle of the present application shall fall within the scope of the claims in the present application.

CLAIMS

1. A method for user authentication, the method comprising:

displaying a picture pre-specified by a first user, the picture comprising a gesture password input interface customized by the first user (S201);

detecting an interactive operation of a second user for the picture (S202);

generating interactive operation information of the second user based on the detected interactive operation of the second user (S203); and

performing authentication to determine whether the second user is the first user by matching the interactive operation information of the second user and standard information, wherein the standard information is generated based on an interactive operation of the first user for the picture (S204),

wherein generating the standard information based on the interactive operation of the first user for the picture comprises:

retrieving the picture specified by the first user (S301);

displaying the picture, and determining one or more feature areas on the picture (S302), wherein determining the one or more feature areas on the picture specifically comprises:

selecting, based on one or more features of the picture, one or more of a plurality of image feature detection algorithms as selected algorithm;

performing feature detection on the picture, and determining the one or more feature areas on the specific picture through feature detection using the selected algorithm; and/or

determining one or more areas specified by the first user on the specific picture, and using the one or more areas as the feature area;

detecting an interactive operation of the first user for the one or more feature areas (S303); and

generating the standard information based on the detected interactive operation of the first user (S304).

2. The method according to claim 1, wherein, before displaying the picture pre-specified by the first user, the method further comprises:

performing setting for the one or more feature areas, wherein setting is used to determine whether to mark the one or more feature areas on the displayed picture pre-specified by the first user.

3. The method according to claim 1, wherein, after determining one or more feature areas on the picture, the method further comprises:

generating corresponding identification information for each feature area.

4. The method according to claim 3, wherein generating the standard information based on the detected interactive operation of the first user comprises:

determining an operation order of the first user for the one or more feature areas based on the detected interactive operation of the first user; and

generating a feature area identification information sequence used to indicate the operation order based on the operation order and identification information corresponding to the one or more feature areas, and using the feature area identification information sequence as the standard information.

5. The method according to claim 4, wherein generating the interactive operation information of the second user based on the detected interactive operation of the second user comprises:

determining an operation order of the second user for the one or more feature areas based on the detected interactive operation of the second user, when it is determined that the interactive operation of the second user comprises an interactive operation of the second user for the one or more feature areas; and

generating a feature area identification information sequence used to indicate the operation order based on the operation order and the identification information corresponding to the one or more feature areas, and using the feature area identification information sequence as the interactive operation information of the second user.

6. The method according to claim 5, wherein performing authentication to determine whether the second user is the first user by matching the interactive operation information of the

second user and standard information specifically comprises:

determining whether the interactive operation information of the second user and the standard information are the same by matching the interactive operation information of the second user and the standard information; and

if yes, authenticating the second user as the first user.

7. The method according to any one of claims 1 to 6, wherein performing the authentication to determine whether the second user is the first user by matching the interactive operation information of the second user and standard information comprises:

determining whether an interactive operation corresponding to the interactive operation information of the second user and an interactive operation corresponding to the standard information are the same by matching the interactive operation information of the second user and the standard information, and if yes, authenticating the second user as the first user; or

determining whether a similarity between an interactive operation corresponding to the interactive operation information of the second user and an interactive operation corresponding to the standard information is not less than a predetermined similarity threshold, by matching the interactive operation information of the second user and the standard information, and if yes, authenticating the second user as the first user.

8. The method according to any one of claims 1 to 7, wherein the interactive operation for the picture comprises at least one of:

a tapping operation for the one or more feature areas on the picture; and

a sliding operation of performing sliding from one feature area to another when there are a plurality of feature areas on the picture.

9. The method according to claim 8, wherein the tapping operation comprises a tapping force, a tapping time, a number of taps, and a tapping frequency.

10. The method according to claim 8, wherein the sliding operation comprises a sliding force, a sliding time, a sliding distance, and a sliding track.

11. An authentication device, for user authentication the device comprising a plurality of modules configured to perform the method of any one of claims 1 to 10.