

# **BIOMETRIC RECOGNITION ATTACK TEST METHODS, APPARATUSES, AND DEVICES**

## **TECHNICAL FIELD**

**[0001]** The present specification relates to the field of computer technologies, and in particular, to biometric recognition attack test methods, apparatuses, and devices.

## **BACKGROUND**

**[0002]** Biometric recognition (for example, fingerprint recognition and palmprint recognition) is usually implemented by using corresponding biometric recognition algorithms. There are many machine learning algorithms applied to the biometric recognition algorithms, and the machine learning algorithms yield more stochastic results.

**[0003]** A biometric recognition capability of a biometric recognition device usually can be manually tested. That is, a plurality of different test volunteers are called up, and then a biometric recognition test is performed on each of the test volunteers until all of the test volunteers complete the test, to obtain a test result. However, there are many machine learning algorithms applied to the biometric recognition algorithms, and the machine learning algorithms yield more stochastic results, and therefore a large quantity of attempts need to be made in the process of testing the biometric recognition capability of the biometric recognition device. Consequently, many human resources need to be consumed, there is a long test period, there are large error variances between manual operations in a manual test, and it is difficult to implement reproduction. Therefore, a better biometric recognition test solution needs to be provided, to more efficiently and accurately test biometric recognition.

## **SUMMARY**

**[0004]** Embodiments of the present specification are intended to provide a better biometric recognition test solution, to more efficiently and accurately test biometric recognition.

**[0005]** To implement the previous technical solution, the embodiments of the present specification are implemented as follows:

**[0006]** Embodiments of the present specification provide a biometric recognition attack test method. The method includes the following: A biometric feature object needed for performing a biometric recognition attack on a biometric recognition device is obtained, where the biometric feature object includes a feature attachment part to which biometric features are attached and a conductive part; a mechanical arm is controlled to place the biometric feature object in a recognition area of the biometric recognition device, and the mechanical arm is controlled to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test; and an attack test result corresponding to the biometric feature object is obtained, and a test result of the biometric recognition attack performed on the biometric recognition device is determined based on the attack test result corresponding to the biometric feature object.

**[0007]** Embodiments of the present specification provide a biometric recognition attack test apparatus. The apparatus includes: an object acquisition module, configured to obtain a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device, where the biometric feature object includes a feature attachment part to which biometric features are attached and a conductive part; an attack test module, configured to control a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and control the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test; and a test result determining module, configured to obtain an attack test result corresponding to the biometric feature object, and determine, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.

**[0008]** Embodiments of the present specification provide a biometric recognition attack test device. The biometric recognition attack test device includes: a processor; and a memory configured to store a computer-executable instruction. When the

executable instruction is executed, the processor is enabled to perform the following operations: obtaining a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device, where the biometric feature object includes a feature attachment part to which biometric features are attached and a conductive part; controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test; and obtaining an attack test result corresponding to the biometric feature object, and determining, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.

**[0009]** Embodiments of the present specification further provide a storage medium. The storage medium is configured to store a computer-executable instruction. When the executable instruction is executed, the following procedures are implemented: obtaining a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device, where the biometric feature object includes a feature attachment part to which biometric features are attached and a conductive part; controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test; and obtaining an attack test result corresponding to the biometric feature object, and determining, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.

## **BRIEF DESCRIPTION OF DRAWINGS**

**[0010]** To describe the technical solutions in the embodiments of the present specification or in the existing technology more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments or the

existing technology. Clearly, the accompanying drawings in the following description are merely some of the embodiments described in the present specification. A person of ordinary skill in the art can further derive other drawings from these accompanying drawings without creative efforts.

[0011] FIG. 1 is an embodiment illustrating a biometric recognition attack test method, according to the present specification;

[0012] FIG. 2A is a schematic structural diagram of a biometric recognition test device, according to the present specification;

[0013] FIG. 2B is a schematic structural diagram of a biometric feature object, according to the present specification;

[0014] FIG. 2C is a schematic structural diagram of a biometric recognition attack test interface, according to the present specification;

[0015] FIG. 3 is an embodiment illustrating another biometric recognition attack test method, according to the present specification;

[0016] FIG. 4 is a schematic diagram illustrating a relationship between an area covered by a biometric feature object in a plurality of different positions and poses and an area corresponding to a biometric recognition attack test, according to the present specification;

[0017] FIG. 5 is an embodiment illustrating a biometric recognition attack test apparatus, according to the present specification; and

[0018] FIG. 6 is an embodiment illustrating a biometric recognition attack test device, according to the present specification.

## **DESCRIPTION OF EMBODIMENTS**

[0019] The embodiments of the present specification provide biometric recognition attack test methods, apparatuses, and devices.

[0020] To make a person skilled in the art better understand the technical solutions in the present specification, the following clearly and comprehensively describes the technical solutions in the embodiments of the present specification with reference to the accompanying drawings in the embodiments of the present specification. Clearly, the described embodiments are merely some but not all of the embodiments of the present specification. All other embodiments obtained by a person of ordinary skill in

the art based on the embodiments of the present specification without creative efforts shall fall within the protection scope of the present specification.

**[0021]** Embodiment 1

**[0022]** As shown in FIG. 1, the embodiments of the present specification provide a biometric recognition attack test method. The method can be performed by a biometric recognition test device. As shown in FIG. 2A, the test device can include a main control child device, a mechanical arm, etc. The main control child device can be a terminal device or a server. The server can be an independent server or a server cluster that includes a plurality of servers. The server can be a back-end server of a financial service, an online shopping service, etc., or can be a back-end server of a certain application program, etc. The terminal device can be a mobile terminal device such as a mobile phone or a tablet computer, or can be a device such as a personal computer. In the embodiments of the present specification, an example in which the main control child device is a terminal device is used for detailed description. For the case of the server, references can be made to the following related content. Details are omitted here for simplicity. The mechanical arm can be connected to the main control child device. The main control child device can send a control instruction to the mechanical arm. The mechanical arm can perform a corresponding operation based on the control instruction. A camera component (for example, a camera) can be disposed on the mechanical arm. The accuracy of the operation of the mechanical arm can be calibrated and fed back by using the camera component, and an object on which an operation is to be performed can be found and determined by using the camera component. The method can specifically include the following steps.

**[0023]** Step S102: Obtain a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device, where the biometric feature object includes a feature attachment part to which biometric features are attached and a conductive part.

**[0024]** The biometric recognition device can be a device that can recognize one or more biometric features. For example, the biometric recognition device can be a fingerprint recognition device or a palmprint recognition device. The fingerprint recognition device can be a device such as an optical fingerprint sensor that obtains a fingerprint image by collecting an optical signal or a capacitive fingerprint sensor that obtains a fingerprint image by collecting a capacitive signal. The biometric recognition device can specifically include but is not limited to a personal computer, a

mobile phone, a trading tool (for example, a vending machine), and various wearable devices (for example, a smart band or a smart watch), or can be another device in which the above sensor is disposed. The biometric recognition attack can be an attack performed on a process of recognizing a biometric feature of a user by using a predetermined recognition method, to verify a recognition capability of the biometric recognition device. For example, an attack is performed on fingerprint recognition performed by the biometric recognition device, to verify a fingerprint recognition capability of the biometric recognition device. For another example, an attack is performed on palmprint recognition performed by the biometric recognition device, to verify a palmprint recognition capability of the biometric recognition device. The biometric recognition attack can be specifically set based on an actual situation. Implementations are not limited in the embodiments of the present specification. The biometric feature object can be a sample or a case object to be used for performing the attack test. There can be one or more biometric feature objects, and each biometric feature object can include a feature attachment part to which biometric features are attached, a conductive part, etc. The conductive part can include a part, made of a conductive material such as conductive ink or conductive silica gel, that can be used for performing a biometric feature test. The conductive part can play a conductive role. The feature attachment part can be a part for carrying biometric features or a part to which biometric features are attached.

**[0025]** In implementation, biometric recognition (for example, fingerprint recognition and palmprint recognition) is usually implemented by using corresponding biometric recognition algorithms. There are many machine learning algorithms applied to the biometric recognition algorithms, and the machine learning algorithms yield more stochastic results. The biometric recognition capability of the biometric recognition device usually can be manually tested. That is, a plurality of different test volunteers are called up, and then a biometric recognition test is performed on each of the test volunteers until all of the test volunteers complete the test, to obtain a test result. However, there are many machine learning algorithms applied to the biometric recognition algorithms, and the machine learning algorithms yield more stochastic results, and therefore a large quantity of attempts need to be made in the process of testing the biometric recognition capability of the biometric recognition device. Consequently, many human resources need to be consumed, there is a long test period, there are large error variances between manual operations in a

manual test, and it is difficult to implement reproduction. Therefore, a better biometric recognition test solution needs to be provided, to more efficiently and accurately test biometric recognition. Embodiments of the present specification provide an implementable technical solution, which can specifically include the following content:

**[0026]** To better perform a biometric recognition attack test, biometric feature images of different test volunteers can be separately collected. For example, for fingerprint recognition, images of a plurality of different fingers of each test volunteer and images of each finger in a plurality of different poses can be separately obtained, and a biometric feature object can be constructed based on the images of each finger in the plurality of different poses. Specifically, paper, a transparent film, etc. used to carry the images are not electrically conductive. When a biometric recognition attack is manually performed, because of conductivity of the finger, a touchscreen of the biometric recognition device can be triggered to perform biometric recognition. However, in the case of a mechanical arm, the touchscreen of the biometric recognition device cannot be triggered to perform biometric recognition. Therefore, corresponding materials can be selected for attaching the biometric feature image, and the selected material can be the feature attachment part. In addition, to enable biometric features in the images to be collected by the biometric recognition device, the conductive part can be disposed. By disposing the conductive part in the biometric feature object, some biometric feature objects that are not electrically conductive and can be only manually tested can be electrically conductive, thereby effectively avoiding phenomena of a long test period, a large test error, etc. in a manual detection process.

**[0027]** It is worthwhile to note that for the above parts and corresponding structures, the feature attachment part and the conductive part be combined (for example, glued together), so that the feature attachment part and the conductive part are combined as a whole to obtain the biometric feature object. In addition, for the above parts and corresponding structures, a substrate can be further disposed. The substrate can combine the feature attachment part and the conductive part as a whole, to obtain the corresponding biometric feature object (as shown in FIG. 2B). The biometric feature object constructed by using the above method can be added to a biometric feature library for storage.

**[0028]** To improve test efficiency, a test interface can be developed in advance by using a corresponding programming language based on processing mechanisms of biometric recognition and a biometric recognition attack test. As shown in FIG. 2C, the test interface can include an input box of information about a biometric recognition device (or user) to be tested, a biometric recognition selection box, test duration, a test start time, a quantity of biometric feature objects, a test result output box, a confirm button, a cancel button, etc. When a biometric recognition attack needs to be performed on a certain biometric recognition device, a tester can determine the biometric recognition device (or corresponding user), and then can obtain related information of the biometric recognition device (or corresponding user), for example, an image or a fingerprint image of the user. The obtained related information can be input into the input box of the information about the biometric recognition device (or user). After the input is completed, the tester can further select, by using the biometric recognition selection box based on an actual situation, a biometric recognition process to be performed, and can set the test duration, the test start time, the quantity of test objects, etc. After the setting is completed, the tester can start a test process, that is, the tester can click the confirm button on the interface. In this case, the test device can obtain the related information of the biometric recognition device to be tested from the input box of the information about the biometric recognition device (or the user), and can further obtain a biometric recognition test type, the test duration, the test start time, the quantity of biometric feature objects, etc. The related information of the biometric recognition device and the other obtained information can be analyzed, to determine a biometric feature object needed for performing a biometric recognition attack on the biometric recognition device.

**[0029]** For example, fingerprint recognition is selected in the biometric recognition selection box, the test start time is a current moment, the test duration and the quantity of test objects do not have to be limited, and the information about the biometric recognition device to be tested can be an identifier such as a name of the biometric recognition device. In this case, the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device can be obtained based on the identifier of the biometric recognition device (or corresponding user).

**[0030]** Step S104: Control the mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and control the mechanical arm to press the biometric feature object to trigger the biometric feature object to

input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test.

**[0031]** The recognition area can be an area in which a biometric feature can be effectively recognized in a process of performing biometric recognition by the biometric recognition device. Fingerprint recognition is used as an example. In this case, an area of the biometric recognition device in which fingerprint data is input can be used as the recognition area. Specifically, the recognition area can be set based on an actual situation. Implementations are not limited in the embodiments of the present specification.

**[0032]** In implementation, after determining the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device, the main control child device in the test device can analyze the obtained biometric feature object, to determine a quantity of included biometric feature objects, and detect current position information of the biometric feature object, and then can send the position information of the biometric feature object to the mechanical arm. The mechanical arm can identify a position of the biometric feature object by using the camera component based on the position information of the biometric feature object, and then the mechanical arm can move to the identified position to pick up the biometric feature object. If there are a plurality of biometric feature objects, the mechanical arm can pick up each biometric feature object, etc. based on a position of the biometric feature object. After the mechanical arm picks up the corresponding biometric feature object, the tester can place or affix the biometric recognition device in a designated position, or the main control child device can send an instruction of setting the biometric recognition device to the mechanical arm. The mechanical arm can identify the biometric recognition device by using the camera component, and then can pick up the biometric recognition device, and place or affix the biometric recognition device in the designated position.

**[0033]** The main control child device can determine the recognition area of the biometric recognition device, and afterwards, can control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device. In this case, although the biometric feature object is placed in the recognition area of the biometric recognition device, if the biometric feature object is not in sufficient contact with the recognition area, the biometric feature object cannot trigger the

biometric recognition device to perform biometric recognition. Based on this, the main control child device can send a control instruction to the mechanical arm to control the mechanical arm to press the biometric feature object. By pressing the biometric feature object, the conductive part in the biometric feature object can trigger the biometric recognition device to perform biometric recognition. In this case, the biometric feature object inputs the biometric feature in the feature attachment part into the biometric recognition device through the conductive part. The biometric recognition device can recognize the biometric feature input by the biometric feature object to obtain a corresponding recognition result.

**[0034]** It is worthwhile to note that the main control child device can further control the mechanical arm to adjust a position and pose of the biometric feature object, so that the biometric feature object can be in a plurality of different positions and poses. The plurality of different positions and poses can be determined based on a plurality of different dimensions, for example, a two-dimensional position and pose, a three-dimensional position and pose, or a five-dimensional position and pose. The position and pose can be specifically set based on an actual situation. Implementations are not limited in the embodiments of the present specification. For each position and pose, the biometric recognition device can start a biometric recognition sensor of the biometric recognition device to collect the biometric feature in the biometric feature object in the recognition area, and can record the recognition result at the same time.

**[0035]** Step S106: Obtain an attack test result corresponding to the biometric feature object, and determine, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.

**[0036]** The test result of the biometric recognition attack performed on the biometric recognition device can include an attack success rate, biometric recognition accuracy, etc. The test result can be specifically set based on an actual situation. Implementations are not limited in the embodiments of the present specification.

**[0037]** In implementation, the attack test result corresponding to the biometric feature object can be obtained from the biometric recognition device, the attack test result corresponding to the biometric feature object (which can include a test result corresponding to the biometric feature object in each position and pose) can be statistically analyzed, to determine a quantity of test results indicating an attack success and a quantity of test results indicating an attack failure, and then the test

result of the biometric recognition attack performed on the biometric recognition device can be determined based on a statistical analysis result. For example, there are 30 biometric feature objects, test results of biometric recognition attacks performed by the test device by controlling the mechanical arm indicate an attack failure for 29 biometric feature objects, and a test result of a biometric recognition attack indicates an attack success for the remaining one biometric feature object. In this case, the test result of the biometric recognition attack performed on the biometric recognition device can include the attack success rate of  $1/30=3.3\%$ , the biometric recognition accuracy of 96.7%, etc.

**[0038]** The embodiments of the present specification provide the biometric recognition attack test method. The biometric feature object needed for performing the biometric recognition attack on the biometric recognition device is obtained, where the biometric feature object includes the feature attachment part to which biometric features are attached and the conductive part; and the mechanical arm is controlled to place the biometric feature object in the recognition area of the biometric recognition device. In this case, the biometric recognition attack test is performed on the biometric recognition device by using the mechanical arm, and therefore human resources are saved. In addition, various parameters (for example, a distance) of the mechanical arm are within a controllable range, thereby reducing an objective error in a manual test. In addition, the mechanical arm can be further controlled to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test; and the attack test result corresponding to the biometric feature object is obtained, and the test result of the biometric recognition attack performed on the biometric recognition device is determined based on the attack test result corresponding to the biometric feature object. In this case, the test is controlled by using the mechanical arm, and therefore test efficiency and test accuracy are improved.

**[0039]** Embodiment 2

**[0040]** As shown in FIG. 3, the embodiments of the present specification provide a biometric recognition attack test method. The method can be performed by a biometric recognition test device. As shown in FIG. 2A, the test device can include a main control child device, a mechanical arm, etc. The main control child device can be a terminal device or a server. The server can be an independent server or a server

cluster that includes a plurality of servers. The server can be a back-end server of a financial service, an online shopping service, etc., or can be a back-end server of a certain application program, etc. The terminal device can be a mobile terminal device such as a mobile phone or a tablet computer, or can be a device such as a personal computer. In the embodiments of the present specification, an example in which the main control child device is a terminal device is used for detailed description. For the case of the server, references can be made to the following related content. Details are omitted here for simplicity. The mechanical arm can be connected to the main control child device. The main control child device can send a control instruction to the mechanical arm. The mechanical arm can perform a corresponding operation based on the control instruction. A camera component (for example, a camera) can be disposed on the mechanical arm. The accuracy of the operation of the mechanical arm can be calibrated and fed back by using the camera component, and an object on which an operation is to be performed can be determined by using the camera component. The method can specifically include the following steps.

**[0041]** Step S302: Obtain an identifier of a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device, where the identifier is set based on a graphic code, and the biometric feature object includes a feature attachment part to which biometric features are attached and a conductive part.

**[0042]** The biometric feature can include at least a fingerprint, a palmprint, etc. The identifier of the biometric feature object can be used to represent information about an identity of the biometric feature object. The identifier of the biometric feature object can be a name, a code, etc. of the biometric feature object. The graphic code can be a barcode, a two-dimensional code, etc.

**[0043]** In implementation, an identifier can be set for each biometric feature object, a corresponding graphic code (for example, a barcode or a two-dimensional code) can be generated by using the identifier, and the generated graphic code can be correspondingly stored with the biometric feature object. Specifically, the generated graphic code can be set on the biometric feature object (for example, the generated graphic code is attached on the biometric feature object). The test device can obtain information about the biometric recognition device to be tested, and can further obtain a biometric recognition test type, test duration, a test start time, a quantity of biometric feature objects, etc. The related information of the biometric recognition device and

the other obtained information can be analyzed, to determine the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device, and the identifier of the determined biometric feature object can be obtained.

**[0044]** Step S304: Control the mechanical arm to obtain a biometric feature object corresponding to the identifier from a feature object library based on the identifier by scanning the graphic code through the camera component disposed on the mechanical arm, and use the obtained biometric feature object as the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device.

**[0045]** The feature object library can be an area for storing different biometric feature objects, a database for storing information about the biometric feature object, etc.

**[0046]** In implementation, when a certain biometric feature object needs to be found or obtained, the camera component disposed on the mechanical arm can be started, a graphic code set on each biometric feature object can be scanned by using the camera component, and an identifier of the biometric feature object corresponding to the graphic code can be determined by analyzing the scanned graphic code. The determined identifier of the biometric feature object can be compared with the obtained identifier of the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device. If the determined identifier of the biometric feature object matches the obtained identifier of the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device, the determined identifier of the biometric feature object can be determined as the identifier of the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device. In this case, the mechanical arm can be controlled to obtain the biometric feature object corresponding to the identifier from the feature object library, and the obtained biometric feature object can be used as the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device. If the determined identifier of the biometric feature object does not match the obtained identifier of the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device, a graphic code of a next biometric feature object can be obtained by using the above method to perform the above processing process, until the

biometric feature object needed for performing the biometric recognition attack on the biometric recognition device is obtained.

**[0047]** It is worthwhile to note that the above implementation is merely an optional implementation, and there can be a plurality of different implementations in practice. Implementations can be specifically set based on an actual situation.

**[0048]** Step S306: Obtain current environmental information, where the environmental information includes one or more of a temperature, humidity, and light intensity.

**[0049]** In addition to the above information, the environmental information can include other related information. The environmental information can be specifically set based on an actual situation.

**[0050]** In implementation, a temperature sensor, a humidity sensor, a light intensity sensor, etc. can be further disposed in the test device. The current temperature, the humidity, and the light intensity can be respectively obtained by the sensors. In other words, the current temperature can be detected by the temperature sensor, the current humidity can be detected by the humidity sensor, and the current light intensity can be detected by the light intensity sensor. The temperature, the humidity, the light intensity, etc. detected by the sensors can be provided for the test device, so that the test device can obtain the current environmental information.

**[0051]** Step S308: Adjust the current environmental information based on predetermined reference environmental information, to obtain environmental information for performing a biometric recognition attack test on the biometric recognition device.

**[0052]** The reference environmental information can be predetermined standard environmental information, and the reference environmental information can vary with the biometric recognition attack test. For example, a fingerprint recognition attack test and a palmprint recognition attack test can correspond to different reference environmental information.

**[0053]** In implementation, a different environment exerts certain impact on biometric recognition, for example, a different temperature exerts impact on sensitivity of a fingerprint recognition component. Specifically, if an environmental temperature is lower than a predetermined temperature threshold, the sensitivity of the fingerprint recognition component is obviously reduced. To eliminate a case in which different biometric recognition attack test results are obtained due to changes in the

environment, uniform environmental information (namely, reference environmental information) can be predetermined. The reference environmental information can be environmental information corresponding to an environment in which least impact is exerted on a biometric recognition component or the biometric recognition component has the best stability, etc. The reference environmental information can be specifically set based on an actual situation.

**[0054]** After the reference environmental information is set by using the above method, when the current environmental information is obtained, the current environmental information can be adjusted by using the reference environmental information, so that the current environmental information matches the reference environmental information. For example, the reference environmental information can include a temperature range of 10°C–25°C, and the current environmental information can include a temperature of –10°C. In this case, the current temperature can be adjusted, so that a value of the temperature falls within the range of 10°C–25°C. Finally, the environmental information for performing the biometric recognition attack test can be obtained. Subsequent processing can be performed based on the environmental information. That is, the environmental information for performing the biometric recognition attack test can be stabilized, and therefore a case in which different biometric recognition attack test results are obtained due to changes in the environment is eliminated.

**[0055]** Step S310: In an environment corresponding to the environmental information for performing the biometric recognition attack test on the biometric recognition device, control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and control the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

**[0056]** In implementation, in the environment corresponding to the environmental information for performing the biometric recognition attack test on the biometric recognition device, the mechanical arm can be controlled to place the biometric feature object in the recognition area of the biometric recognition device, and the mechanical arm can be controlled to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part

into the biometric recognition device through the conductive part, to perform the biometric recognition attack test. For a specific processing process of step S310 of controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test, references can be made to the specific processing process of step S104 in Embodiment 1. Details are omitted here for simplicity.

**[0057]** In addition, the specific processing process of step S310 does not have to be limited to the specific processing process of step S104 in Embodiment 1, and can be implemented by using plurality of other different methods. Specific processing of controlling the mechanical arm to press the biometric feature object in step 310 can be implemented by using a plurality of different methods. An optional processing method is provided below, and can specifically include the following content: The mechanical arm is controlled to press the biometric feature object based on a predetermined pressure parameter. The pressure parameter includes a pressure force parameter and a pressure angle parameter used by the mechanical arm to press the biometric feature object.

**[0058]** In implementation, reference values corresponding to the pressure force parameter and the pressure angle parameter used by the mechanical arm to press the biometric feature object can be set based on an actual situation, and the pressure parameter for pressing the biometric feature object can be set based on the determined reference values corresponding to the pressure force parameter and the pressure angle parameter. When the mechanical arm needs to be controlled to simulate a finger or palm to input the biometric feature into the biometric recognition device, the determined pressure parameter can be provided for the mechanical arm, and the mechanical arm can press the biometric feature object by using the obtained pressure parameter. The biometric feature in the biometric feature object is input into the biometric recognition device by setting the same pressure parameter, and therefore consistency of input variables of biometric feature objects can be ensured when the biometric feature objects perform the biometric recognition attack test, to improve accuracy of the attack test performed on the biometric recognition device, and

accuracy can also be ensured when test results corresponding to the plurality of biometric feature objects are compared.

**[0059]** In addition, a specific processing process of controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device in step S 310 can be implemented by using a plurality of different methods. Three optional processing methods are provided below, and can specifically include the following methods 1 to 3.

**[0060]** Method 1: The mechanical arm is controlled, by using the camera component and a predetermined image recognition algorithm, to place the biometric feature object in the recognition area of the biometric recognition device. For specific processing, references can be made to processing of the following step A2 to step A6.

**[0061]** Step A2: Obtain a first image that includes the recognition area of the biometric recognition device and a second image that includes the biometric feature object through the camera component disposed on the mechanical arm.

**[0062]** In implementation, the camera component (for example, a camera) can be disposed on the mechanical arm, the camera component disposed on the mechanical arm can be started, and the first image that includes the recognition area of the biometric recognition device and a predetermined reference position can be captured. Similarly, the second image that includes the biometric feature object and the predetermined reference position can be captured.

**[0063]** Step A4: Separately determine position information of the recognition area relative to the predetermined reference position and position information of the biometric feature object relative to the predetermined reference position based on the obtained first image, the obtained second image, and the predetermined image recognition algorithm.

**[0064]** The position information of the recognition area relative to the predetermined reference position can be two-dimensional position information, three-dimensional position information, geographical location information, etc. The position information of the recognition area relative to the predetermined reference position can be specifically set based on an actual situation.

**[0065]** In implementation, the first image and the second image can be separately analyzed by using the predetermined image recognition algorithm, to determine related information such as a shape and a size of the recognition area and related information such as a shape and a size of the biometric feature object, and to further

determine the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position. In a process of capturing the first image and the second image by the camera component disposed on the mechanical arm, different objects (including the recognition area of the biometric recognition device, the biometric feature object, the predetermined reference position, etc.) in the first image and the second image can be marked by different colors or other marking methods, and the predetermined reference position, the recognition area, and a distance between the predetermined reference position and the biometric feature object can be marked by using different colors or other marking methods. For example, two-dimensional axis information can be marked by using a special color range. For example, the two-dimensional axis information can be indicated by using a white bounding box or a black bounding box, a position of the biometric feature object can be indicated by using a green bounding box, a position of the biometric feature in the biometric feature object can be indicated by using a red bounding box, a position of the recognition area of the biometric recognition device can be indicated by using a blue bounding box, and a position of the graphic code in the biometric feature object can be indicated by using a yellow bounding box. This can be specifically set based on an actual situation. Implementations are not limited in the embodiments of the present specification. As such, three-dimensional positions of the recognition area of the biometric recognition device and the biometric feature object can be completely identified by using a combination of two-dimensional images and colors, so that a movement trajectory can be planned for the mechanical arm, and the recognition area of the biometric recognition device and the biometric feature object can be accurately located.

**[0066]** Step A6: Control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device based on the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position.

**[0067]** In implementation, after the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position are obtained by using the above method, the movement trajectory of the mechanical arm can be

planned based on the position information. The planned movement trajectory then can be provided for the mechanical arm, and the mechanical arm can pick up the biometric feature object, and place the biometric feature object in the recognition area of the biometric recognition device.

**[0068]** Method 2: The biometric feature object further includes a positioning part, and the mechanical arm is controlled to place the biometric feature object in the recognition area of the biometric recognition device by using the positioning part. For specific processing, references can be made to processing of the following step B2 to step B8.

**[0069]** Step B2: Send a positioning signal to each of the positioning part of the biometric feature object and the biometric recognition device.

**[0070]** The biometric recognition device can also include a positioning part, and the positioning part can be a positioning part of a predetermined positioning system (for example, a positioning part of a GPS or a positioning part of a Beidou navigation satellite system), can be a positioning part implemented based on a millimeter wave, Wi-Fi, Bluetooth, NFC, etc., or can be specifically set based on an actual situation. Implementations are not limited in the embodiments of the present specification. The positioning signal can include, for example, an identifier of the test device, a current time, the positioning part of the biometric feature object, and an identifier of the biometric recognition device, or can be specifically set based on an actual situation. Implementations are not limited in the embodiments of the present specification.

**[0071]** Step B4: Receive a response signal, corresponding to the positioning signal, returned by each of the positioning part of the biometric feature object and the biometric recognition device.

**[0072]** The response signal can include, for example, the identifier of the test device, a time of sending the response signal, the positioning part of the biometric feature object, and the identifier of the biometric recognition device, or can be specifically set based on an actual situation. Implementations are not limited in the embodiments of the present specification.

**[0073]** Step B6: Separately determine position information of the recognition area relative to a predetermined reference position and position information of the biometric feature object relative to the predetermined reference position based on related information corresponding to the positioning signal and the response signal.

**[0074]** In implementation, the test device can calculate a relative distance between the recognition area and the predetermined reference position and a relative distance between the biometric feature object and the predetermined reference position based on the related information corresponding to the positioning signal and the response signal (for example, the current time in the positioning signal and the time of sending the response signal in the response signal), a signal propagation speed, etc., and can further determine the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position.

**[0075]** Step B8: Control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device based on the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position.

**[0076]** For a specific processing process of step B8, references can be made to the specific processing process of step A6 in method 1. Details are omitted here for simplicity.

**[0077]** Method 3: The mechanical arm is controlled to place the biometric feature object in the recognition area of the biometric recognition device based on a plurality of position adjustments by using the camera component and a predetermined image recognition algorithm. For specific processing, references can be made to processing of the following step C2 and step C4.

**[0078]** Step C2: Control the mechanical arm to place the biometric feature object in a preselected area, where the preselected area is an area that includes or is adjacent to the recognition area of the biometric recognition device.

**[0079]** In implementation, the mechanical arm can be controlled to randomly place the biometric feature object in the area that includes the recognition area of the biometric recognition device, or the mechanical arm can be controlled to randomly place the biometric feature object in the adjacent area of the recognition area, to reduce processing pressure of the test device at a certain time point.

**[0080]** Step C4: Control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device by moving the biometric feature object towards the recognition area at least once based on the camera

component disposed on the mechanical arm and the predetermined image recognition algorithm.

**[0081]** In implementation, the camera component disposed on the mechanical arm can be started to capture an image that includes the recognition area of the biometric recognition device and the biometric feature object, and the captured image can be analyzed by using the predetermined image recognition algorithm to determine whether the biometric feature object is placed in the recognition area of the biometric recognition device. If it is determined that the biometric feature object is not placed in the recognition area of the biometric recognition device, the test device can control the mechanical arm to move the biometric feature object towards the recognition area of the biometric recognition device at a predetermined step distance (for example, 1 cm or 5 mm). Then, the camera component disposed on the mechanical arm can be started again to capture an image that includes the recognition area of the biometric recognition device and the biometric feature object, and the captured image can be analyzed by using the predetermined image recognition algorithm to determine whether the biometric feature object is placed in the recognition area of the biometric recognition device. If it is determined that the biometric feature object is placed in the recognition area of the biometric recognition device, subsequent processing can be continued. If it is determined that the biometric feature object is not placed in the recognition area of the biometric recognition device, the test device can control the mechanical arm to continue to move the biometric feature object towards the recognition area of the biometric recognition device at the predetermined step distance. The processing then can be repeated, until the biometric feature object is placed in the recognition area of the biometric recognition device.

**[0082]** A specific processing process of step C4 can be implemented by using a plurality of different methods. One optional processing method is provided below, and can specifically include processing in the following steps C42 to C46.

**[0083]** Step C42: Obtain the image that includes the biometric feature object and the recognition area through the camera component disposed on the mechanical arm.

**[0084]** Step C44: Determine positional relationship information between the biometric feature object and the recognition area by using the predetermined image recognition algorithm based on the obtained image that includes the biometric feature object and the recognition area.

**[0085]** The positional relationship information between the biometric feature object and the recognition area can include, for example, a relative distance range between the biometric feature object and the recognition area and information indicating whether the biometric feature object is located in the recognition area. The positional relationship information can be specifically set based on an actual situation. Implementations are not limited in the embodiments of the present specification.

**[0086]** Step C46: Determine, based on the determined positional relationship information, a distance at which the biometric feature object moves towards the recognition area, and control the mechanical arm to move the biometric feature object towards the recognition area based on the determined distance.

**[0087]** In implementation, the distance at which the biometric feature object moves towards the recognition area can be determined based on the relative distance range, between the biometric feature object and the recognition area, in the determined positional relationship information. For example, the relative distance range between the biometric feature object and the recognition area is 1 cm to 3 cm. In this case, it can be determined that the distance at which the biometric feature object moves towards the recognition area is 1 cm (or 2 cm, 1.5 cm, etc.), and then the mechanical arm can be controlled to move the biometric feature object towards the recognition area based on the determined distance of 1 cm.

**[0088]** After the above processing, the processing in step C42 to step C46 can be repeated, until the biometric feature object is placed in the recognition area of the biometric recognition device.

**[0089]** Alternatively, specific processing of step S310 can be implemented by using the following method, which can specifically include processing in step D2 and D4.

**[0090]** Step D2: Control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and control the mechanical arm to adjust a position and pose of the biometric feature object in the recognition area of the biometric recognition device.

**[0091]** The position and pose of the biometric feature object in the recognition area of the biometric recognition device can refer to a position, a placement pose, etc. The position can be geographical location coordinates, coordinates corresponding to a coordinate system that is established by using a certain point or surface as a starting point or a starting surface and set based on an actual situation, etc. The placement pose can be an inclined pose, a horizontal pose, an inverted pose, etc. The position

and pose can be specifically set based on an actual situation. Implementations are not limited in the embodiments of the present specification.

**[0092]** In implementation, the main control child device can determine the recognition area of the biometric recognition device, and afterwards, can control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device. In this case, the test device can control the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test, and can record a test result. The main control child device can further control the mechanical arm to adjust the position and pose of the biometric feature object, so that the biometric feature object can be in a plurality of different positions and poses. The plurality of different positions and poses can be determined based on a plurality of different dimensions, for example, a two-dimensional position and pose, a three-dimensional position and pose, or a five-dimensional position and pose. The position and pose can be specifically set based on an actual situation. Implementations are not limited in the embodiments of the present specification.

**[0093]** Step D4: In each adjusted position and pose of the biometric feature object in the recognition area of the biometric recognition device, control the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

**[0094]** Based on the above processing, the position and pose of the biometric feature object in the recognition area of the biometric recognition device can be automatically and dynamically adjusted. A test range can cover an entire trajectory range of the biometric feature object by performing a plurality of attack tests. A position of the biometric feature object in the recognition area of the biometric recognition device can be adjusted, so that a ratio of the test range to the trajectory range of the biometric feature object can be dynamically adjusted. For details, references can be made to the following related content: An area covered by the biometric feature object in the plurality of different positions and poses is greater than or equal to an area corresponding to the biometric recognition attack test.

**[0095]** As shown in FIG. 4, a plurality of circular areas are the trajectory range of the biometric feature object, and the test range is a range of a rectangular area. Clearly, the area covered by the biometric feature object in the plurality of different positions and poses is greater than or equal to the area corresponding to the biometric recognition attack test. As such, test accuracy and comprehensiveness can be improved.

**[0096]** In addition, if an attack test result corresponding to a first biometric feature object is an attack success, where the first biometric feature object is any biometric feature object, processing in step E2 to step E6 can be performed on the first biometric feature object.

**[0097]** Step E2: Obtain position information of the first biometric feature object in a biometric recognition attack test performed based on the first biometric feature object.

**[0098]** In implementation, the test device can control the camera component disposed on the mechanical arm to capture an image that includes the first biometric feature object in the biometric recognition attack test performed based on the first biometric feature object, and can analyze the image by using a predetermined image recognition algorithm to obtain the position information of the first biometric feature object in the biometric recognition attack test performed based on the first biometric feature object.

**[0099]** Step E4: Control, based on the position information of the first biometric feature object, the mechanical arm to repeat the biometric recognition attack test by using the first biometric feature object, and obtain an attack test result corresponding to the biometric recognition attack test repeated by using the first biometric feature object.

**[0100]** In implementation, a placement position of the first biometric feature object is determined based on the position information of the first biometric feature object (the placement position can be the same as a position corresponding to the position information of the first biometric feature object, or can be a position obtained by adjusting a position corresponding to the position information of the first biometric feature object by using a predetermined position adjustment method). Then, the mechanical arm can be controlled to re-place the biometric feature object in the recognition area of the biometric recognition device, and the mechanical arm is controlled to press the biometric feature object to trigger the biometric feature object

to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test. In addition, the attack test result corresponding to the biometric recognition attack test repeated by using the first biometric feature object can be obtained.

**[0101]** Step E6: Use the obtained attack test result corresponding to the biometric recognition attack test repeated by using the first biometric feature object as the attack test result corresponding to the biometric feature object.

**[0102]** Step S312: Obtain the attack test result corresponding to the biometric feature object, and determine, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.

**[0103]** It is worthwhile to note that when there are a plurality of biometric feature objects, the processing in step 302 to step 312 can be repeatedly performed for each biometric feature object. Finally, the test result of the biometric recognition attack performed on the biometric recognition device can be determined based on an attack test result corresponding to each biometric feature object.

**[0104]** The embodiments of the present specification provide the biometric recognition attack test method. The biometric feature object needed for performing the biometric recognition attack on the biometric recognition device is obtained, where the biometric feature object includes the feature attachment part to which biometric features are attached and the conductive part; and the mechanical arm is controlled to place the biometric feature object in the recognition area of the biometric recognition device. In this case, the biometric recognition attack test is performed on the biometric recognition device by using the mechanical arm, and therefore human resources are saved. In addition, various parameters (for example, a distance) of the mechanical arm are within a controllable range, thereby reducing an objective error in a manual test. In addition, the mechanical arm can be further controlled to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test; and the attack test result corresponding to the biometric feature object is obtained, and the test result of the biometric recognition attack performed on the biometric recognition device is determined based on the attack test result corresponding to the biometric feature

object. In this case, the test is controlled by using the mechanical arm, and therefore test efficiency and test accuracy are improved.

**[0105]** In addition, a change between a plurality of poses and a plurality of positions and poses can be implemented by using the mechanical arm to implement an automatic biometric recognition test, so that a problem in the biometric recognition process can be easily reproduced and human resources in the test can be saved.

**[0106]** Embodiment 3

**[0107]** The biometric recognition attack test method provided in the embodiments of the present specification is described above. Based on the same idea, embodiments of the present specification further provide a biometric recognition attack test apparatus, as shown in FIG. 5.

**[0108]** The biometric recognition attack test apparatus includes an object acquisition module 501, an attack test module 502, and a test result determining module 503.

**[0109]** The object acquisition module 501 is configured to obtain a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device. The biometric feature object includes a feature attachment part to which biometric features are attached and a conductive part.

**[0110]** The attack test module 502 is configured to control a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and control the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test.

**[0111]** The test result determining module 503 is configured to obtain an attack test result corresponding to the biometric feature object, and determine, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.

**[0112]** In the embodiments of the present specification, the apparatus further includes:

**[0113]** an environmental information acquisition module, configured to obtain current environmental information, where the environmental information includes one or more of a temperature, humidity, and light intensity; and

**[0114]** an environment adjustment module, configured to adjust the current environmental information based on predetermined reference environmental information, to obtain environmental information for performing the biometric recognition attack test on the biometric recognition device; and

**[0115]** the attack test module 502 is configured to: in an environment corresponding to the environmental information for performing the biometric recognition attack test on the biometric recognition device, control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and control the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

**[0116]** In the embodiments of the present specification, the attack test module 502 includes:

**[0117]** a position and pose adjustment unit, configured to control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and control the mechanical arm to adjust a position and pose of the biometric feature object in the recognition area of the biometric recognition device; and

**[0118]** a first attack test unit, configured to: in each adjusted position and pose of the biometric feature object in the recognition area of the biometric recognition device, control the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

**[0119]** In the embodiments of the present specification, the attack test module 502 is configured to control the mechanical arm to press the biometric feature object based on a predetermined pressure parameter. The pressure parameter includes a pressure force parameter and a pressure angle parameter used by the mechanical arm to press the biometric feature object.

**[0120]** In the embodiments of the present specification, the attack test module 502 includes:

**[0121]** an image acquisition unit, configured to obtain a first image that includes the recognition area of the biometric recognition device and a second image that

includes the biometric feature object through a camera component disposed on the mechanical arm;

**[0122]** a first position determining unit, configured to separately determine position information of the recognition area relative to a predetermined reference position and position information of the biometric feature object relative to the predetermined reference position based on the obtained first image, the obtained second image, and a predetermined image recognition algorithm; and

**[0123]** a first control unit, configured to control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device based on the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position.

**[0124]** In the embodiments of the present specification, the biometric feature object further includes a positioning part, and the attack test module 502 includes:

**[0125]** a signal sending unit, configured to send a positioning signal to each of the positioning part of the biometric feature object and the biometric recognition device;

**[0126]** a response receiving unit, configured to receive a response signal, corresponding to the positioning signal, returned by each of the positioning part of the biometric feature object and the biometric recognition device;

**[0127]** a second position determining unit, configured to separately determine position information of the recognition area relative to a predetermined reference position and position information of the biometric feature object relative to the predetermined reference position based on related information corresponding to the positioning signal and the response signal; and

**[0128]** a second control unit, configured to control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device based on the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position.

**[0129]** In the embodiments of the present specification, the attack test module 502 includes:

**[0130]** a third control unit, configured to control the mechanical arm to place the biometric feature object in a preselected area, where the preselected area is an area

that includes or is adjacent to the recognition area of the biometric recognition device;  
and

**[0131]** a second attack test unit, configured to control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device by moving the biometric feature object towards the recognition area at least once based on a camera component disposed on the mechanical arm and a predetermined image recognition algorithm.

**[0132]** In the embodiments of the present specification, the second attack test unit is configured to obtain an image that includes the biometric feature object and the recognition area through the camera component disposed on the mechanical arm; determine positional relationship information between the biometric feature object and the recognition area by using the predetermined image recognition algorithm based on the obtained image that includes the biometric feature object and the recognition area; and determine, based on the determined positional relationship information, a distance at which the biometric feature object moves towards the recognition area, and control the mechanical arm to move the biometric feature object towards the recognition area based on the determined distance.

**[0133]** In the embodiments of the present specification, the object acquisition module 501 includes:

**[0134]** an identifier acquisition unit, configured to obtain an identifier of the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device, where the identifier is set based on a graphic code; and

**[0135]** an object acquisition unit, configured to control the mechanical arm to obtain a biometric feature object corresponding to the identifier from a feature object library based on the identifier by scanning the graphic code through the camera component disposed on the mechanical arm, and using the obtained biometric feature object as the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device.

**[0136]** In the embodiments of the present specification, if an attack test result corresponding to a first biometric feature object is an attack success, where the first biometric feature object is any biometric feature object, the apparatus further includes:

**[0137]** a component position acquisition module, configured to obtain position information of the first biometric feature object in a biometric recognition attack test performed based on the first biometric feature object;

**[0138]** a test repeat module, configured to control, based on the position information of the first biometric feature object, the mechanical arm to repeat the biometric recognition attack test by using the first biometric feature object, and obtain an attack test result corresponding to the biometric recognition attack test repeated by using the first biometric feature object; and

**[0139]** A result determining module, configured to use the obtained attack test result corresponding to the biometric recognition attack test repeated by using the first biometric feature object as the attack test result corresponding to the biometric feature object.

**[0140]** In the embodiments of the present specification, the biometric feature includes at least a fingerprint and a palmprint.

**[0141]** The embodiments of the present specification provide the biometric recognition attack test apparatus. The biometric feature object needed for performing the biometric recognition attack on the biometric recognition device is obtained, where the biometric feature object includes the feature attachment part to which biometric features are attached and the conductive part; and the mechanical arm is controlled to place the biometric feature object in the recognition area of the biometric recognition device. In this case, the biometric recognition attack test is performed on the biometric recognition device by using the mechanical arm, and therefore human resources are saved. In addition, various parameters (for example, a distance) of the mechanical arm are within a controllable range, thereby reducing an objective error in a manual test. In addition, the mechanical arm can be further controlled to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test; and the attack test result corresponding to the biometric feature object is obtained, and the test result of the biometric recognition attack performed on the biometric recognition device is determined based on the attack test result corresponding to the biometric feature object. In this case, the test is controlled by using the mechanical arm, and therefore test efficiency and test accuracy are improved.

**[0142]** In addition, a change between a plurality of poses and a plurality of positions and poses can be implemented by using the mechanical arm to implement an automatic biometric recognition test, so that a problem in the biometric recognition process can be easily reproduced and human resources in the test can be saved.

**[0143]** Embodiment 4

**[0144]** The biometric recognition attack test apparatus provided in the embodiments of the present specification is described above. Based on the same idea, the embodiments of the present specification further provide a biometric recognition attack test device, as shown in FIG. 6.

**[0145]** The biometric recognition attack test device can be the biometric recognition test device provided in the above embodiments. The test device can include a main control child device, a mechanical arm, etc. The main control child device can be a terminal device or a server. The server can be an independent server or a server cluster that includes a plurality of servers. The server can be a back-end server of a financial service, an online shopping service, etc., or can be a back-end server of a certain application program, etc. The terminal device can be a mobile terminal device such as a mobile phone or a tablet computer, or can be a device such as a personal computer.

**[0146]** The biometric recognition attack test device can vary with configuration or performance, and can include one or more processors 601 and a memory 602. The memory 602 can store one or more memory application programs or data. The memory 602 can be transient or persistent storage. The application program stored in the memory 602 can include one or more modules (not shown in the figure). Each module can include a series of computer-executable instructions for the biometric recognition attack test device. Further, the processor 601 can be configured to communicate with the memory 602 to execute the series of computer-executable instructions in the memory 602 on the biometric recognition attack test device. The biometric recognition attack test device can further include one or more power supplies 603, one or more wired or wireless network interfaces 604, one or more input/output interfaces 605, one or more keyboards 606, and a mechanical arm 606.

**[0147]** Specifically, in the embodiments, the biometric recognition attack test device includes a memory and one or more programs. The one or more programs are stored in the memory. The one or more programs can include one or more modules, and each module can include a series of computer-executable instructions for the biometric recognition attack test device. One or more processors are configured to execute the computer-executable instructions included in each module in the one or more programs, to perform the following operations:

**[0148]** obtaining a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device, where the biometric feature object includes a feature attachment part to which biometric features are attached and a conductive part;

**[0149]** controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test; and

**[0150]** obtaining an attack test result corresponding to the biometric feature object, and determining, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.

**[0151]** In the embodiments of the present specification, the following operations are further included:

**[0152]** obtaining current environmental information, where the environmental information includes one or more of a temperature, humidity, and light intensity; and

**[0153]** adjusting the current environmental information based on predetermined reference environmental information, to obtain environmental information for performing the biometric recognition attack test on the biometric recognition device; and

**[0154]** the controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test includes:

**[0155]** in an environment corresponding to the environmental information for performing the biometric recognition attack test on the biometric recognition device, controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the

biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

**[0156]** In the embodiments of the present specification, the controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test includes:

**[0157]** controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and controlling the mechanical arm to adjust a position and pose of the biometric feature object in the recognition area of the biometric recognition device; and

**[0158]** in each adjusted position and pose of the biometric feature object in the recognition area of the biometric recognition device, controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

**[0159]** In the embodiments of the present specification, the controlling the mechanical arm to press the biometric feature object includes:

**[0160]** controlling the mechanical arm to press the biometric feature object based on a predetermined pressure parameter, where the pressure parameter includes a pressure force parameter and a pressure angle parameter used by the mechanical arm to press the biometric feature object.

**[0161]** In the embodiments of the present specification, the controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device includes:

**[0162]** obtaining a first image that includes the recognition area of the biometric recognition device and a second image that includes the biometric feature object through a camera component disposed on the mechanical arm;

**[0163]** separately determining position information of the recognition area relative to a predetermined reference position and position information of the biometric feature object relative to the predetermined reference position based on the obtained first image, the obtained second image, and a predetermined image recognition algorithm; and

**[0164]** controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device based on the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position.

**[0165]** In the embodiments of the present specification, the biometric feature object further includes a positioning part, and the controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device includes:

**[0166]** sending a positioning signal to each of the positioning part of the biometric feature object and the biometric recognition device;

**[0167]** receiving a response signal, corresponding to the positioning signal, returned by each of the positioning part of the biometric feature object and the biometric recognition device;

**[0168]** separately determining position information of the recognition area relative to a predetermined reference position and position information of the biometric feature object relative to the predetermined reference position based on related information corresponding to the positioning signal and the response signal; and

**[0169]** controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device based on the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position.

**[0170]** In the embodiments of the present specification, the controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device includes:

**[0171]** controlling the mechanical arm to place the biometric feature object in a preselected area, where the preselected area is an area that includes or is adjacent to the recognition area of the biometric recognition device; and

**[0172]** controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device by moving the biometric feature object towards the recognition area at least once based on a camera component disposed on the mechanical arm and a predetermined image recognition algorithm.

**[0173]** In the embodiments of the present specification, the controlling the mechanical arm to move the biometric feature object towards the recognition area at least once based on a camera component disposed on the mechanical arm and a predetermined image recognition algorithm includes:

**[0174]** obtaining an image that includes the biometric feature object and the recognition area through the camera component;

**[0175]** determining positional relationship information between the biometric feature object and the recognition area by using the predetermined image recognition algorithm based on the obtained image that includes the biometric feature object and the recognition area; and

**[0176]** determining, based on the determined positional relationship information, a distance at which the biometric feature object moves towards the recognition area, and controlling the mechanical arm to move the biometric feature object towards the recognition area based on the determined distance.

**[0177]** In the embodiments of the present specification, the obtaining a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device includes:

**[0178]** obtaining an identifier of the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device, where the identifier is set based on a graphic code; and

**[0179]** controlling the mechanical arm to obtain a biometric feature object corresponding to the identifier from a feature object library based on the identifier by scanning the graphic code through the camera component disposed on the mechanical arm, and using the obtained biometric feature object as the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device.

**[0180]** In the embodiments of the present specification, if an attack test result corresponding to a first biometric feature object is an attack success, where the first biometric feature object is any biometric feature object, the following operations are further included:

**[0181]** obtaining position information of the first biometric feature object in a biometric recognition attack test performed based on the first biometric feature object;

**[0182]** controlling, based on the position information of the first biometric feature object, the mechanical arm to repeat the biometric recognition attack test by using the

first biometric feature object, and obtaining an attack test result corresponding to the biometric recognition attack test repeated by using the first biometric feature object; and

**[0183]** using the obtained attack test result corresponding to the biometric recognition attack test repeated by using the first biometric feature object as the attack test result corresponding to the biometric feature object.

**[0184]** In the embodiments of the present specification, the biometric feature includes at least a fingerprint and a palmprint.

**[0185]** The embodiments of the present specification provide the biometric recognition attack test device. The biometric feature object needed for performing the biometric recognition attack on the biometric recognition device is obtained, where the biometric feature object includes the feature attachment part to which biometric features are attached and the conductive part; and the mechanical arm is controlled to place the biometric feature object in the recognition area of the biometric recognition device. In this case, the biometric recognition attack test is performed on the biometric recognition device by using the mechanical arm, and therefore human resources are saved. In addition, various parameters (for example, a distance) of the mechanical arm are within a controllable range, thereby reducing an objective error in a manual test. In addition, the mechanical arm can be further controlled to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test; and the attack test result corresponding to the biometric feature object is obtained, and the test result of the biometric recognition attack performed on the biometric recognition device is determined based on the attack test result corresponding to the biometric feature object. In this case, the test is controlled by using the mechanical arm, and therefore test efficiency and test accuracy are improved.

**[0186]** In addition, a change between a plurality of poses and a plurality of positions and poses can be implemented by using the mechanical arm to implement an automatic biometric recognition test, so that a problem in the biometric recognition process can be easily reproduced and human resources in the test can be saved.

**[0187]** Embodiment 5

**[0188]** Further, based on the methods shown in FIG. 1 to FIG. 4, one or more embodiments of the present specification further provide a storage medium

configured to store computer-executable instruction information. In a specific embodiment, the storage medium can be a USB flash drive, an optical disc, a hard disk, etc. When the computer-executable instruction information stored in the storage medium is executed by a processor, the following procedures can be implemented:

**[0189]** obtaining a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device, where the biometric feature object includes a feature attachment part to which biometric features are attached and a conductive part;

**[0190]** controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test; and

**[0191]** obtaining an attack test result corresponding to the biometric feature object, and determining, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.

**[0192]** In the embodiments of the present specification, the following operations are further included:

**[0193]** obtaining current environmental information, where the environmental information includes one or more of a temperature, humidity, and light intensity; and

**[0194]** adjusting the current environmental information based on predetermined reference environmental information, to obtain environmental information for performing the biometric recognition attack test on the biometric recognition device; and

**[0195]** the controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test includes:

**[0196]** in an environment corresponding to the environmental information for performing the biometric recognition attack test on the biometric recognition device,

controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

**[0197]** In the embodiments of the present specification, the controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test includes:

**[0198]** controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and controlling the mechanical arm to adjust a position and pose of the biometric feature object in the recognition area of the biometric recognition device; and

**[0199]** in each adjusted position and pose of the biometric feature object in the recognition area of the biometric recognition device, controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

**[0200]** In the embodiments of the present specification, the controlling the mechanical arm to press the biometric feature object includes:

**[0201]** controlling the mechanical arm to press the biometric feature object based on a predetermined pressure parameter, where the pressure parameter includes a pressure force parameter and a pressure angle parameter used by the mechanical arm to press the biometric feature object.

**[0202]** In the embodiments of the present specification, the controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device includes:

**[0203]** obtaining a first image that includes the recognition area of the biometric recognition device and a second image that includes the biometric feature object through a camera component disposed on the mechanical arm;

**[0204]** separately determining position information of the recognition area relative to a predetermined reference position and position information of the biometric

feature object relative to the predetermined reference position based on the obtained first image, the obtained second image, and a predetermined image recognition algorithm; and

**[0205]** controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device based on the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position.

**[0206]** In the embodiments of the present specification, the biometric feature object further includes a positioning part, and the controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device includes:

**[0207]** sending a positioning signal to each of the positioning part of the biometric feature object and the biometric recognition device;

**[0208]** receiving a response signal, corresponding to the positioning signal, returned by each of the positioning part of the biometric feature object and the biometric recognition device;

**[0209]** separately determining position information of the recognition area relative to a predetermined reference position and position information of the biometric feature object relative to the predetermined reference position based on related information corresponding to the positioning signal and the response signal; and

**[0210]** controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device based on the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position.

**[0211]** In the embodiments of the present specification, the controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device includes:

**[0212]** controlling the mechanical arm to place the biometric feature object in a preselected area, where the preselected area is an area that includes or is adjacent to the recognition area of the biometric recognition device; and

**[0213]** controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device by moving the biometric feature

object towards the recognition area at least once based on a camera component disposed on the mechanical arm and a predetermined image recognition algorithm.

**[0214]** In the embodiments of the present specification, the controlling the mechanical arm to move the biometric feature object towards the recognition area at least once based on a camera component disposed on the mechanical arm and a predetermined image recognition algorithm includes:

**[0215]** obtaining an image that includes the biometric feature object and the recognition area through the camera component;

**[0216]** determining positional relationship information between the biometric feature object and the recognition area by using the predetermined image recognition algorithm based on the obtained image that includes the biometric feature object and the recognition area; and

**[0217]** determining, based on the determined positional relationship information, a distance at which the biometric feature object moves towards the recognition area, and controlling the mechanical arm to move the biometric feature object towards the recognition area based on the determined distance.

**[0218]** In the embodiments of the present specification, the obtaining a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device includes:

**[0219]** obtaining an identifier of the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device, where the identifier is set based on a graphic code; and

**[0220]** controlling the mechanical arm to obtain a biometric feature object corresponding to the identifier from a feature object library based on the identifier by scanning the graphic code through the camera component disposed on the mechanical arm, and using the obtained biometric feature object as the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device.

**[0221]** In the embodiments of the present specification, if an attack test result corresponding to a first biometric feature object is an attack success, where the first biometric feature object is any biometric feature object, the following operations are further included:

**[0222]** obtaining position information of the first biometric feature object in a biometric recognition attack test performed based on the first biometric feature object;

**[0223]** controlling, based on the position information of the first biometric feature object, the mechanical arm to repeat the biometric recognition attack test by using the first biometric feature object, and obtaining an attack test result corresponding to the biometric recognition attack test repeated by using the first biometric feature object; and

**[0224]** using the obtained attack test result corresponding to the biometric recognition attack test repeated by using the first biometric feature object as the attack test result corresponding to the biometric feature object.

**[0225]** In the embodiments of the present specification, the biometric feature includes at least a fingerprint and a palmprint.

**[0226]** The embodiments of the present specification provide the storage medium. The biometric feature object needed for performing the biometric recognition attack on the biometric recognition device is obtained, where the biometric feature object includes the feature attachment part to which biometric features are attached and the conductive part; and the mechanical arm is controlled to place the biometric feature object in the recognition area of the biometric recognition device. In this case, the biometric recognition attack test is performed on the biometric recognition device by using the mechanical arm, and therefore human resources are saved. In addition, various parameters (for example, a distance) of the mechanical arm are within a controllable range, thereby reducing an objective error in a manual test. In addition, the mechanical arm can be further controlled to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test; and the attack test result corresponding to the biometric feature object is obtained, and the test result of the biometric recognition attack performed on the biometric recognition device is determined based on the attack test result corresponding to the biometric feature object. In this case, the test is controlled by using the mechanical arm, and therefore test efficiency and test accuracy are improved.

**[0227]** In addition, a change between a plurality of poses and a plurality of positions and poses can be implemented by using the mechanical arm to implement an automatic biometric recognition test, so that a problem in the biometric recognition process can be easily reproduced and human resources in the test can be saved.

**[0228]** Specific embodiments of the present specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps described in the claims can be performed in a sequence different from that in the embodiments, and the desired results can still be achieved. In addition, the process described in the accompanying drawings does not necessarily require a particular sequence or sequential sequence shown to achieve the desired results. In some implementations, multi-tasking and parallel processing can be advantageous.

**[0229]** In the 1990s, whether a technical improvement is a hardware improvement (for example, an improvement of a circuit structure, such as a diode, a transistor, or a switch) or a software improvement (an improvement of a method procedure) can be clearly distinguished. However, as technologies develop, current improvements of many method procedures can be considered as direct improvements of hardware circuit structures. A designer usually programs an improved method procedure into a hardware circuit, to obtain a corresponding hardware circuit structure. Therefore, a method procedure can be improved by using a hardware entity module. For example, a programmable logic device (PLD) (for example, a field programmable gate array (FPGA)) is such an integrated circuit, and a logical function of the PLD is determined by a user through device programming. The designer performs programming to "integrate" a digital system to a PLD without requesting a chip manufacturer to design and produce an application-specific integrated circuit chip. In addition, the programming is mostly implemented by modifying "logic compiler" software instead of manually making an integrated circuit chip. This is similar to a software compiler used for program development and compiling. However, original code before compiling is also written in a specific programming language, which is referred to as a hardware description language (HDL). There are many HDLs, such as an Advanced Boolean Expression Language (ABEL), an Altera Hardware Description Language (AHDL), Confluence, a Cornell University Programming Language (CUPL), HDCal, a Java Hardware Description Language (JHDL), Lava, Lola, MyHDL, PALASM, and a Ruby Hardware Description Language (RHDL). Currently, a Very-High-Speed Integrated Circuit Hardware Description Language (VHDL) and Verilog are most commonly used. A person skilled in the art should also understand that a hardware circuit that implements a logical method procedure can be readily obtained once the method procedure is logically programmed by using the several described hardware description languages and is programmed into an integrated circuit.

**[0230]** A controller can be implemented by using any appropriate method. For example, the controller can be a microprocessor or a processor, a computer-readable medium that stores computer readable program code (such as software or firmware) that can be executed by a microprocessor or a processor, a logic gate, a switch, an application-specific integrated circuit (ASIC), a programmable logic controller, or a built-in microprocessor. Examples of the controller include but are not limited to the following microprocessors: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20, and Silicone Labs C8051F320. The memory controller can also be implemented as a part of control logic of a memory. A person skilled in the art also knows that, in addition to implementing the controller by using the computer readable program code, logic programming can be performed on method steps to allow the controller to implement the same function in forms of a logic gate, a switch, an application-specific integrated circuit, a programmable logic controller, and a built-in microcontroller. Therefore, the controller can be considered as a hardware component, and an apparatus configured to implement various functions in the controller can also be considered as a structure in the hardware component. Or the apparatus configured to implement various functions can even be considered as both a software module implementing the method and a structure in the hardware component.

**[0231]** The system, apparatus, module, or unit illustrated in the previously described embodiments can be specifically implemented by a computer chip or an entity, or can be implemented by a product having a certain function. A typical implementation device is a computer. The computer can be, for example, a personal computer, a laptop computer, a cellular phone, a camera phone, a smartphone, a personal digital assistant, a media player, a navigation device, an email device, a game console, a tablet computer, or a wearable device, or a combination of any of these devices.

**[0232]** For ease of description, the apparatus above is described by dividing functions into various units. Certainly, when one or more embodiments of the present specification are implemented, function of units can be implemented in one or more pieces of software and/or hardware.

**[0233]** A person skilled in the art should understand that the embodiments of the present specification can be provided as methods, systems, or computer program products. Therefore, one or more embodiments of the present specification can use a form of hardware only embodiments, software only embodiments, or embodiments

with a combination of software and hardware. In addition, one or more embodiments of the present specification 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 disk memory, a CD-ROM, an optical memory, etc.) that include computer-usable program code.

**[0234]** The embodiments of the present specification are described with reference to the flowcharts and/or block diagrams of the method, the device (system), and the computer program product based on the embodiments of the present specification. 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 processes and/or blocks 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 biometric recognition attack test device to generate a machine, so that the instructions executed by the computer or the processor of the another programmable biometric recognition attack test 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.

**[0235]** These computer program instructions can be stored in a computer readable memory that can instruct a computer or another programmable biometric recognition attack test device to work in a specific way, 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.

**[0236]** These computer program instructions can be loaded onto a computer or another programmable biometric recognition attack test 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 the 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.

**[0237]** In a typical configuration, a computing device includes one or more processors (CPUs), input/output interfaces, network interfaces, and memories.

**[0238]** The memory can include a non-persistent memory, 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.

**[0239]** The computer-readable medium includes persistent, non-persistent, removable, and irremovable media that can store information by using any method or technology. The information can be a computer readable instruction, a data structure, a program module, or other data. Examples of a computer storage medium include but are not limited to a parameter random access memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), another type of random access memory (RAM), a read-only memory (ROM), 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 other optical storage, a cassette magnetic tape, magnetic tape/magnetic disk storage or another magnetic storage device, or any other non-transmission medium. The computer storage medium can be used to store information accessible by a computing device. Based on the definition in the present specification, the computer-readable medium does not include transitory computer readable media (transitory media) such as a modulated data signal and carrier.

**[0240]** It is worthwhile to further note that the terms "include", "comprise", and their any other variants are intended to cover a nonexclusive inclusion, so that a process, a method, a product, or a device that includes a series of elements not only includes these elements, but also includes other elements which are not expressly listed, or further includes elements inherent to such process, method, product, or device. An element described by "includes a ..." further includes, without more constraints, another same or identical element in the process, method, product, or device that includes the element.

**[0241]** A person skilled in the art should understand that the embodiments of the present specification can be provided as methods, systems, or computer program products. Therefore, one or more embodiments of the present specification can use a form of hardware only embodiments, software only embodiments, or embodiments with a combination of software and hardware. In addition, one or more embodiments of the present specification 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 disk memory, a CD-ROM, an optical memory, etc.) that include computer-usable program code.

**[0242]** One or more embodiments of the present specification can be described in the general context of computer-executable instructions executed by a computer, for example, a program module. The program module usually includes a routine, a program, an object, a component, a data structure, etc. for executing a specific task or implementing a specific abstract data type. One or more embodiments of the present specification can be practiced in distributed computing environments. In the distributed computing environments, tasks are performed by remote processing devices that are connected through a communications network. In the distributed computing environment, the program module can be located in both local and remote computer storage media including storage devices.

**[0243]** The embodiments of the present specification are described in a progressive way. For same or similar parts in the embodiments, references can be made to these embodiments, and each embodiment focuses on a difference from other embodiments. Particularly, the system embodiment is basically similar to the method embodiments, and therefore is described briefly. For related parts, references can be made to partial description in the method embodiments.

**[0244]** The previous descriptions are merely embodiments of the present specification, and are not intended to limit the present specification. For a person skilled in the art, the present specification can have various modifications and changes. Any modifications, equivalent replacements, and improvements made within the spirit and the principle of the present specification shall fall within the scope of the claims in the present specification.

## CLAIMS

What is claimed is:

1. A biometric recognition attack test method, wherein the method comprises:

obtaining a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device, wherein the biometric feature object comprises a feature attachment part to which biometric features are attached and a conductive part;

controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test; and

obtaining an attack test result corresponding to the biometric feature object, and determining, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.

2. The method according to claim 1, wherein the method further comprises:

obtaining current environmental information, wherein the environmental information comprises one or more of a temperature, humidity, and light intensity; and

adjusting the current environmental information based on predetermined reference environmental information, to obtain environmental information for performing the biometric recognition attack test on the biometric recognition device; and

the controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test comprises:

in an environment corresponding to the environmental information for performing the biometric recognition attack test on the biometric recognition device,

controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

3. The method according to claim 1 or 2, wherein the controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test comprises:

controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and controlling the mechanical arm to adjust a position and pose of the biometric feature object in the recognition area of the biometric recognition device; and

in each adjusted position and pose of the biometric feature object in the recognition area of the biometric recognition device, controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

4. The method according to claim 3, wherein the controlling the mechanical arm to press the biometric feature object comprises:

controlling the mechanical arm to press the biometric feature object based on a predetermined pressure parameter, wherein the pressure parameter comprises a pressure force parameter and a pressure angle parameter used by the mechanical arm to press the biometric feature object.

5. The method according to claim 4, wherein the controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device comprises:

obtaining a first image that comprises the recognition area of the biometric recognition device and a second image that comprises the biometric feature object through a camera component disposed on the mechanical arm;

separately determining position information of the recognition area relative to a predetermined reference position and position information of the biometric

feature object relative to the predetermined reference position based on the obtained first image, the obtained second image, and a predetermined image recognition algorithm; and

controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device based on the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position.

6. The method according to claim 4, wherein the biometric feature object further comprises a positioning part, and the controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device comprises:

sending a positioning signal to each of the positioning part of the biometric feature object and the biometric recognition device;

receiving a response signal, corresponding to the positioning signal, returned by each of the positioning part of the biometric feature object and the biometric recognition device;

separately determining position information of the recognition area relative to a predetermined reference position and position information of the biometric feature object relative to the predetermined reference position based on related information corresponding to the positioning signal and the response signal; and

controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device based on the position information of the recognition area relative to the predetermined reference position and the position information of the biometric feature object relative to the predetermined reference position.

7. The method according to claim 4, wherein the controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device comprises:

controlling the mechanical arm to place the biometric feature object in a preselected area, wherein the preselected area is an area that comprises or is adjacent to the recognition area of the biometric recognition device; and

controlling the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device by moving the biometric feature

object towards the recognition area at least once based on a camera component disposed on the mechanical arm and a predetermined image recognition algorithm.

8. The method according to claim 7, wherein the controlling the mechanical arm to move the biometric feature object towards the recognition area at least once based on a camera component disposed on the mechanical arm and a predetermined image recognition algorithm comprises:

- obtaining an image that comprises the biometric feature object and the recognition area through the camera component;

- determining positional relationship information between the biometric feature object and the recognition area by using the predetermined image recognition algorithm based on the obtained image that comprises the biometric feature object and the recognition area; and

- determining, based on the determined positional relationship information, a distance at which the biometric feature object moves towards the recognition area, and controlling the mechanical arm to move the biometric feature object towards the recognition area based on the determined distance.

9. The method according to claim 1, wherein the obtaining a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device comprises:

- obtaining an identifier of the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device, wherein the identifier is set based on a graphic code; and

- controlling the mechanical arm to obtain a biometric feature object corresponding to the identifier from a feature object library based on the identifier by scanning the graphic code through the camera component disposed on the mechanical arm, and using the obtained biometric feature object as the biometric feature object needed for performing the biometric recognition attack on the biometric recognition device.

10. The method according to claim 1, wherein if an attack test result corresponding to a first biometric feature object is an attack success, wherein the first biometric feature object is any biometric feature object, the method further comprises:

- obtaining position information of the first biometric feature object in a biometric recognition attack test performed based on the first biometric feature object;

controlling, based on the position information of the first biometric feature object, the mechanical arm to repeat the biometric recognition attack test by using the first biometric feature object, and obtaining an attack test result corresponding to the biometric recognition attack test repeated by using the first biometric feature object; and

using the obtained attack test result corresponding to the biometric recognition attack test repeated by using the first biometric feature object as the attack test result corresponding to the biometric feature object.

11. The method according to claim 1, wherein the biometric feature comprises at least a fingerprint and a palmprint.

12. A biometric recognition attack test apparatus, wherein the apparatus comprises:

an object acquisition module, configured to obtain a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device, wherein the biometric feature object comprises a feature attachment part to which biometric features are attached and a conductive part;

an attack test module, configured to control a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and control the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test; and

a test result determining module, configured to obtain an attack test result corresponding to the biometric feature object, and determine, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.

13. The apparatus according to claim 12, wherein the apparatus further comprises:

an environmental information acquisition module, configured to obtain current environmental information, wherein the environmental information comprises one or more of a temperature, humidity, and light intensity; and

an environment adjustment module, configured to adjust the current environmental information based on predetermined reference environmental

information, to obtain environmental information for performing the biometric recognition attack test on the biometric recognition device; and

the attack test module is configured to: in an environment corresponding to the environmental information for performing the biometric recognition attack test on the biometric recognition device, control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and control the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

14. The apparatus according to claim 12 or 13, wherein the attack test module comprises:

a position and pose adjustment unit, configured to control the mechanical arm to place the biometric feature object in the recognition area of the biometric recognition device, and control the mechanical arm to adjust a position and pose of the biometric feature object in the recognition area of the biometric recognition device; and

a first attack test unit, configured to: in each adjusted position and pose of the biometric feature object in the recognition area of the biometric recognition device, control the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform the biometric recognition attack test.

15. The apparatus according to claim 14, wherein the attack test module is configured to control the mechanical arm to press the biometric feature object based on a predetermined pressure parameter, wherein the pressure parameter comprises a pressure force parameter and a pressure angle parameter used by the mechanical arm to press the biometric feature object.

16. The apparatus according to claim 12, wherein the biometric feature comprises at least a fingerprint and a palmprint.

17. A biometric recognition attack test device, wherein the biometric recognition attack test device comprises:

a processor; and

a memory configured to store a computer-executable instruction, wherein when the executable instruction is executed, the processor is enabled to perform the following operations:

- obtaining a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device, wherein the biometric feature object comprises a feature attachment part to which biometric features are attached and a conductive part;

- controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test; and

- obtaining an attack test result corresponding to the biometric feature object, and determining, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.

18. A storage medium, wherein the storage medium is configured to store a computer-executable instruction, and when the executable instruction is executed, the following procedures are implemented:

- obtaining a biometric feature object needed for performing a biometric recognition attack on a biometric recognition device, wherein the biometric feature object comprises a feature attachment part to which biometric features are attached and a conductive part;

- controlling a mechanical arm to place the biometric feature object in a recognition area of the biometric recognition device, and controlling the mechanical arm to press the biometric feature object to trigger the biometric feature object to input the biometric feature in the feature attachment part into the biometric recognition device through the conductive part, to perform a biometric recognition attack test; and

- obtaining an attack test result corresponding to the biometric feature object, and determining, based on the attack test result corresponding to the biometric feature object, a test result of the biometric recognition attack performed on the biometric recognition device.