

BIOMETRIC AUTHENTICATION, IDENTIFICATION AND DETECTION METHOD AND DEVICE FOR MOBILE TERMINAL DEVICE AND EQUIPMENT

Technical Field

5 [01] The present application relates to the field of computer software technologies, and in particular to a biometric authentication, identification and detection method and device for a mobile terminal device, and an electronic device.

Background

10 [02] The security of a biometric authentication system in use has always been an issue that attracts widespread attention.

[03] Taking a face recognition system as an example, the most common spoofing method in the face recognition system is impersonation attack or reproduction attack. Namely, an imposter uses a fake feature having the same expression form to invade the system. At present,
15 commonly used means for impersonation attack mainly include photos (or processed images), videos, 3D models, and the like.

[04] Impersonation attacks to face recognition systems are mainly addressed by using liveness detection technologies. Existing liveness detection methods include 3D depth information analysis, detection of physiological behaviors like blink, facial expression and speech
20 interaction, Fourier frequency analysis, thermal infrared radiation (IR), and the like. The detection of physiological behaviors like blink and the facial expression and speech interaction typically require a user to blink, open mouth, or read a randomly generated speech. These liveness detection methods are effective, but depend on cooperation by the user.

25 Summary

[05] The objective of embodiments of the present application is to provide a biometric authentication, identification and detection method and apparatus for a mobile terminal device, and an electronic device, which can reduce the dependence on user cooperation or do not depend on user cooperation to achieve the effect of strengthening the security of biometric
30 authentication and identification. The embodiments of the present application provide better security support for users while enhancing user experience.

[06] To solve the above technical problems, the embodiments of the present application are implemented as follows.

[07] According to a first aspect, a biometric authentication, identification and detection method

for a mobile terminal device is provided, and the method comprises:

[08] obtaining sensor data of the mobile terminal device when the mobile terminal device performs biometric authentication and identification; and

[09] determining whether an attack occurs based on the sensor data and an attack
5 determination model;

[10] where the attack determination model is obtained based on training with sensor training data.

[11] According to a second aspect, a biometric authentication, identification, and detection apparatus is provided, and the device comprises:

10 [12] an obtaining unit configured to obtain sensor data of a mobile terminal device when the mobile terminal device performs biometric authentication and identification; and

[13] an attack determining unit configured to determine whether an attack occurs based on the sensor data and an attack determination model;

[14] where the attack determination model is obtained based on training with sensor
15 training data.

[15] According to a third aspect, an electronic device is provided, comprising:

[16] a processor; and

[17] a memory configured to store computer executable instructions, where the executable instructions cause, when executed, the processor to execute the following operations:

20 [18] obtaining sensor data of a mobile terminal device when the mobile terminal device performs biometric authentication and identification; and

[19] determining whether an attack occurs based on the sensor data and an attack determination model;

[20] where the attack determination model is obtained based on training with sensor
25 training data.

[21] According to a fourth aspect, a computer readable storage medium is provided, where the computer readable storage medium stores one or more programs, and the one or more programs, when executed by an electronic device comprising a plurality of applications, cause the electronic device to execute the following operations:

30 [22] obtaining sensor data of a mobile terminal device when the mobile terminal device performs biometric authentication and identification; and

[23] determining whether an attack occurs based on the sensor data and an attack determination model;

[24] where the attack determination model is obtained based on training with sensor

training data.

[25] From the technical solutions provided by the embodiments of the present application, it can be seen that the technical solutions according to the embodiments of the present application can at least achieve one of the following technical effects.

- 5 [26] Sensor data collected by a mobile terminal device during biometric authentication and identification is obtained, and attack determination is performed on the sensor data based on a sensor classification model. As a result, with reduced dependence or without dependence on user cooperation, the effect of strengthening the security of biometric authentication and identification can be achieved. The embodiments of the present application provide better
10 security support for users while enhancing user experience.

Brief Description of the Drawings

- [27] To more clearly describe the technical solutions of the embodiments of the present application or of the current technologies, the accompanying drawings to be used in the
15 description of the embodiments or the current technologies will be briefly described below. Apparently, the accompanying drawings in the description below are merely some of the embodiments of the present application. Other drawings may be obtained by one of ordinary skill in the art without creative effort according to these accompanying drawings.

- [28] FIG. 1 is a flow chart of a biometric authentication, identification and detection
20 method for a mobile terminal device according to some embodiments of the present application.

[29] FIG. 2 is a flow chart of interactions in biometric authentication, identification and detection by a mobile terminal device according to some embodiments of the present application.

- 25 [30] FIG. 3 is a schematic flow chart of training and prediction for biometric authentication and identification according to some embodiments of the present application.

[31] FIG. 4 is a schematic structural diagram of an electronic device according to some embodiments of the present application.

- [32] FIG. 5 is a schematic structural diagram of a biometric authentication, identification,
30 and detection apparatus according to some embodiments of the present application.

Detailed Description

[33] To enable those skilled in the art to better understand the technical solutions of the present application, the technical solutions of the embodiments of the present application will

be completely and thoroughly described below with reference to the accompanying drawings in the embodiments of the present application. Apparently, the described embodiments are merely some, but not all, embodiments of the present application. All other embodiments obtained, based on some embodiments of the present application, by one of ordinary skill in the art without creative effort shall fall within the protection scope of the present application.

[34] FIG. 1 is a flow chart of a biometric authentication, identification and detection method for a mobile terminal device according to some embodiments of the present application. The method shown in FIG. 1 may be implemented by a biometric authentication, identification, and detection apparatus or a biometric authentication, identification and detection application on the mobile terminal device. In other words, the method shown in FIG. 1 may be implemented by the mobile terminal device.

[35] S110, obtaining sensor data of a mobile terminal device when the mobile terminal device performs biometric authentication and identification.

[36] It should be understood that, in the embodiments of the present application, there may be various authentication and identification methods for biometric authentication and identification, such as facial feature authentication and identification, speech feature authentication and identification, gesture input feature authentication and identification, etc. The solutions of the embodiments of the present application may be applicable to various biometric authentication and identification, which is not limited by the embodiments of the present application.

[37] It should be understood that the time length for collecting the sensor data may be the same or different for users having different risk levels. Optionally, in the step S110, a desired time length for collecting the sensor data may be determined based on a risk level of a user. A higher risk level requires a longer time length for sensor data collection. For example, it is assumed that user risk levels are divided into three types, i.e., low risk users, regular risk users, and high risk users. For users at a low risk level, it may be prescribed that the collection time length is 3 seconds; for users at a regular risk level, it may be prescribed that the collection time length is 5 seconds; for users at a low risk level, it may be prescribed that the collection time length is 7 seconds, and the like.

[38] FIG. 2 is a schematic diagram of a six-dimensional parameter of the mobile terminal device according to some embodiments of the present application. It should be understood that a three-axis gyroscope may sense comprehensive dynamic information of the mobile terminal device, including left and right angle of inclination (roll), front and back angle of inclination (pitch), and left and right swing angle (yaw), respectively; and a three-axis accelerator may

sense acceleration of the mobile terminal device in three directions in a 3D space (x-axis, y-axis, and z-axis) and three directions of front and back, left and right, and up and down. The three-axis gyroscope is configured to detect angular rotation and balance, and data measured thereby may be referred to as gyroscope data. The three-axis accelerator is configured to detect lateral acceleration, and data measured thereby may be referred to as acceleration sensor data. The three-axis gyroscope and the three-axis accelerator may be collectively referred to as a six-axis gyroscope.

[39] It should be understood that, when the sensor data of the mobile terminal device is obtained in the embodiments of the present application, the gyroscope data and/or the acceleration sensor data as shown in FIG. 2 may be obtained.

[40] S120, determining whether an attack occurs based on the sensor data and an attack determination model.

[41] Here, the attack determination model is obtained based on training with sensor training data.

[42] It should be understood that, when the user performs biometric authentication and identification in the embodiments of the present application, sensor data may be different for a normal user and an imposter user. Taking face authentication and identification as an example, if the imposter user performs authentication and identification by a photo (or a processed image), a video, a 3D model, or other impersonation attack means, the sensor data at the time of authentication thereof is apparently different from sensor data at the time of authentication and identification by the normal user. On the basis of this concept, whether an attack occurs during the process of biometric authentication and identification corresponding to the sensor data may be determined based on the sensor data and an attack determination model.

[43] It should be understood that, to determine whether an attack occurs based on the sensor data and an attack determination model may, for example, use the sensor data as an input to the attack determination model, so as to determine whether an attack occurs, or to perform data processing on the sensor data to obtain processed sensor data, and then use the processed sensor data as an input to the attack determination model to determine whether an attack occurs.

[44] For example, an output result of the attack determination model may be a probability that an attack occurs, a range of probabilities that an attack occurs, a risk level of attack occurrence, or straightly be whether an attack occurs. Based on the output result, it may be directly determined whether an attack occurs. Alternatively, based on certain conversion processing on the output result, it may be determined whether an attack occurs. Alternatively,

based on the output result and in combination with other factors like models and rules, it may be determined whether an attack occurs. A probability segmentation of the attack determination model and risk levels of attack occurrence are listed in Table 1.

Table 1

Model probability segmentation	Risk levels of attack occurrence
[0.5, 1]	Ultra-high risk
[0.4, 0.5]	High risk
[0.3, 0.4]	Medium risk
[0, 0.3]	Low risk

5

[45] According to practical online testing, when a determination threshold is set to 0.4 (i.e., it is determined that an attack occurs when the probability is greater than 0.4 and no attack occurs when the probability is lower than 0.4), the number of times of identifying a risk accounts for one ten-thousandth of the total number of times of invocation; most of the times of identifying a risk are attack attempts according to manual verification, and the number of times of misjudgment accounts for three hundred-thousandth of the total number of times of invocation.

10

[46] In the embodiments of the present application, sensor data collected by a mobile terminal device during biometric authentication and identification is obtained, and attack determination is performed on the sensor data based on a sensor classification model. As a result, with reduced dependence or without dependence on user cooperation, the effect of strengthening the security of biometric authentication and identification can be achieved. The embodiments of the present application provide better security support for users while enhancing user experience.

15

[47] It should be understood that, in the step S120, data processing may be performed on the sensor data, and the sensor data after the data processing may be used as an input to the attack determination model.

20

[48] Optionally, the step S120 may comprise: pre-processing the sensor data to obtain pre-processed sensor data, where the pre-processing comprises at least one of the following: filtering operation, boundary detection operation, and length normalization operation; and

25

[49] determining whether an attack occurs based on the pre-processed sensor data and the attack determination model;

[50] where the attack determination model is obtained based on training with the pre-processed sensor training data.

[51] These three pre-processing methods will be described briefly as follows.

[52] Filtering processing:

5 [53] Since noises due to shaky hands or inherent to the sensors themselves are mostly with high-frequency data, filtering processing is often performed first when data pre-processing is performed. In the embodiments of the present application, a low-pass filter may be used to suppress data with high frequencies. In addition, a moving average method may be adopted in the embodiments of the present application to process the sensor data. For example, taking
10 acceleration data on the x-axis as an example, the processing may be performed using the following equation:

$$acc_x[i] = \frac{1}{M} \sum_{j=0}^{M-1} acc_x[i-j]$$

[54] where acc_x represents acceleration data on the x-axis, and M represents the size of a moving window.

15 [55] The processing of acceleration data on the x-axis may be referenced for similar processing on acceleration data on the y-axis and z-axis and gyroscope data on the x, y, and z axes, which will not be elaborated.

[56] At the same time, assuming that an output from the acceleration sensor comprises gravitational acceleration, a high-pass filter may be used to remove the gravitational impact, or
20 a linear acceleration sensor may be directly used to replace the regular acceleration sensor.

[57] It should be understood that the filtering processing in the embodiments of the present application is merely exemplary, while other filtering processing methods are not excluded. For example, a variable sliding smoothing algorithm may be adopted for processing, etc.

[58] (2) Boundary detection processing:

25 [59] For example, time points at which the user starts and ends the biometric authentication and identification may be identified by a threshold method based on an added window. One time window is used from the front and back ends of the sensor data, respectively, to explore toward the middle. If the variation of the sensor values in one time window exceeds a threshold, then the first frame corresponding to the time window used to
30 explore from the front to the back is recorded as a beginning boundary, the last frame corresponding to the time window used to explore from the back to the front is recorded as an

ending boundary, and the beginning boundary and the ending boundary are used to define a beginning frame and an ending frame of the biometric authentication and identification. Similarly, other boundary detection processing methods are not excluded in the process of boundary detection processing, either.

5 [60] (3) Length normalization processing:

[61] By the normalization processing, the original data with inconsistent variation lengths is processed to obtain data with a consistent variation length. 3D interactions based on the sensor mutually depend on amplitude and changing speed of actions of the user of the mobile terminal device, a data sequence, and changes to the data sequence appear to have inconsistent
10 lengths, leading to discontinuous changes of 3D scenes and jitter in the data.

[62] There are many methods for length normalization.

[63] If the sensor has been smoothed, the linear difference method may be adopted in the length normalization processing on the sensor data. A result of the linear difference may effectively fill up blanks among discontinuous data points, and the complexity of the
15 calculation is low, which takes the processor performance of the mobile terminal device into consideration at the same time.

[64] For example, Y value at a position X in the interval $[X_0, X_1]$ is obtained by using the coordinates of starting points of the discontinuous data (X_0, Y_0) , (X_1, Y_1) , based on an exemplary equation as follows:

20
$$Y = Y_0 + \frac{(X - X_0)}{(X_1 - X_0)}(Y_1 - Y_0).$$

[65] The above equation is merely exemplary and may be modified to a certain extent.

[66] Furthermore, in addition to the linear difference method, there are many normalization methods. For example, the sensor data in the first direction of X, Y, and Z axes may be used as a normalization standard, and the sensor data in the other two directions may
25 be converted according to the first direction, so as to determine the coordinate points corresponding to the normalized data.

[67] For example, $X = X_0 + nD_x$; $Y = Y_0 + nD_y$; $Z = Z_0 + nD_z$.

[68] Here, D_x is a distance on the X axis between two adjacent normalized coordinate points, D_y is a distance on the Y axis between two adjacent normalized coordinate points, and
30 D_z is a distance on the Z axis between two adjacent normalized coordinate points.

[69] In the embodiments of the present application, by performing data pre-processing on the sensor data to eliminate noises due to shaky hands or inherent to the sensors themselves during sensor data collection, the sensor data with relatively high confidence may then be

obtained.

[70] It should be understood that, in addition to performing data pre-processing on the sensor data before using an attack determination model for attack determination, the sensor data may also be pre-processed before training the attack determination model based on sensor training data, so as to obtain the sensor training data.

[71] Optionally, the step S120 may comprise:

[72] performing feature extraction based on the sensor data to obtain the sensor data with features extracted; and

[73] determining whether an attack occurs based on the sensor data with features extracted and the attack determination model;

[74] where the attack determination model is obtained based on training with sensor training data with features extracted.

[75] It should be understood that, in the embodiments of the present application, the sensor data before the feature extraction may be the pre-processed sensor data or may be the sensor data of the mobile terminal device when the mobile terminal device performs biometric authentication and identification, which is not limited in the embodiments of the present application.

[76] For example, the sensor data with features extracted comprises the acceleration sensor data of the mobile terminal device and/or the gyroscope data of the mobile terminal device, where,

[77] the acceleration sensor data comprises one or more pieces of the following data: an average, a standard deviation, a median, a maximum, a minimum, and an integral of the acceleration sensor of the mobile terminal device in three directions of x, y, and z axes; and

[78] the gyroscope data comprises one or more pieces of the following data:

[79] an average, a standard deviation, a median, a maximum, a minimum, and an integral of the gyroscope of the mobile terminal device in three directions of x, y, and z axes.

[80] It should be understood that, in the embodiments of the present application, the integral is used to represent the speed and displacement of the mobile terminal device.

[81] It should be understood that the time length for performing the biometric authentication and identification is also an important parameter of the sensor data. In the embodiments of the present application, the sensor data serving as an input to the attack determination model may further comprise the time length for performing the biometric authentication and identification.

[82] The data processing methods before the sensor data is input to the attack

determination model are listed above. It should be understood that the above-described pre-processing operation and feature extraction operation are optional.

[83] It should be understood that, before the attack determination model is used to perform determination on the sensor, training based on a large amount of sensor training data needs to be performed to obtain the attack determination model. The above-described data processing methods may also be applied in the training phase of the attack determination model to perform data processing based on the sensor data to obtain sensor training data for training the attack determination model.

[84] Optionally, before the step S110, the method may further comprise:

[85] obtaining sensor data of the mobile terminal device collected when the mobile terminal device performed biometric authentication and identification historically to obtain multiple sets of sensor training data for the mobile terminal device; and

[86] using the multiple sets of sensor training data as inputs to the attack determination model for training to obtain the attack determination model.

[87] As described above, in the embodiments of the present application, data processing operations, such as pre-processing, feature extraction, and the like, may be performed on the sensor data collected during biometric authentication and identification to obtain the sensor training data.

[88] It should be understood that supervised binary classification model training or unsupervised binary classification model training may be adopted during the model training.

[89] With regard to the supervised model training, training samples with concept labels (classifications) need to be learned, so as to predict labels (classifications) of data outside of the training sample set as much as possible. In other words, when the sensor data is input for model training, the input sensor data needs to be labeled as sensor data with an attack occurring or sensor data without an attack. For example, label (classification) prediction needs to be performed on an output result corresponding to the input sensor data. Algorithms for supervised training of the model may comprise all regression algorithms and classification algorithms, such as linear regression, decision tree, neural network, K-Nearest Neighbor (KNN), Support Vector Machine (SVM), etc.

[90] At this point, before the step S110, the method may further comprise:

[91] obtaining sensor data of the mobile terminal device collected when the mobile terminal device performed biometric authentication and identification historically;

[92] determining sensor training data and a corresponding label based on the sensor data and corresponding attack occurrence situation, the label used for indicating whether an attack

has occurred to the corresponding sensor training data; and

[93] using multiple sets of sensor training data and corresponding labels as inputs to the attack determination model for training to obtain the attack determination model.

[94] It should be understood that, in the embodiments of the present application, the multiple sets of sensor training data may comprise sensor training data labeled as attack occurring and/or sensor training data labeled as attack not occurring.

[95] There are many training algorithms for supervised training of the model, and different training algorithms have different parameters set for the training of the model. The Random Forest algorithm (Random Forrest) is taken as an example of functions. In a particular example, main parameter settings in the attack determination model may comprise the following: the number of decision trees is 100, the minimum number of leaf nodes is 100, etc. It should be understood that these parameter settings are adjustable.

[96] With regard to the unsupervised model training, training samples without concept labels (classifications) need to be learned, so as to find structural knowledge in the training sample set. In the unsupervised model training, all labels (classifications) are unknown. Algorithms for unsupervised training of the model may comprise all clustering algorithms, such as k-means, Principal Component Analysis (PCA), gaussian mixture model (GMM), etc.

[97] At this point, before the step S110, the method may further comprise:

[98] obtaining sensor data of the mobile terminal device collected when the mobile terminal device performed biometric authentication and identification historically;

[99] determining sensor training data based on the sensor data; and

[100] using multiple sets of sensor training data as inputs to the attack determination model for performing clustering training on the multiple sets of historical sensor data to obtain the attack determination model.

[101] It should be understood that, during the model training, the training may also be performed based on sensor data of different user risk levels and/or different mobile terminal device models to obtain an attack determination model capable of supporting different user risk levels and/or different mobile terminal device models.

[102] Optionally, as an exemplary embodiment, the method may further comprise: obtaining a risk level of a user corresponding to the mobile terminal device and/or model data of the mobile terminal device;

[103] where the step S120 may be, for example, implemented as follows:

[104] determining whether an attack occurs based on the risk level of a user corresponding to the mobile terminal device and/or model data of the mobile terminal device, the sensor data

and the attack determination model;

[105] where the training of the attack determination model further uses sensor training data corresponding to the risk level of the user of the mobile terminal device and/or the model of the mobile terminal device.

5 [106] For example, taking the supervised model training as an example, in addition to using the sensor training data as an input feature during the model training, the risk level of the user corresponding to the sensor data may also be used as an input feature, the model of the mobile terminal device corresponding to the sensor data may be used as an input feature, the risk level of the user and the model of the mobile terminal device corresponding to the sensor data may
10 be both used as input features, or the like.

[107] For example, it is assumed that user risk levels are divided into three types, i.e., low risk users, regular risk users, and high risk users. During the attack model training, the attack determination model may be trained based on sensor training data corresponding to these three risk levels. Accordingly, when attack determination and detection is performed, the sensor
15 training data needs to be used as input features of the attack determination model, and moreover, the user risk level corresponding to the sensor training data also needs to be used as an input feature of the attack determination model to determine whether an attack occurs.

[108] The method for training the attack determination model according to sensor training data of mobile terminal devices of different models is similar to the method for training the
20 attack determination model according to the user risk level, which will not be elaborated here.

[109] It should be understood that, in exemplary applications, the mobile terminal device model and the user risk level may be both used as input features of the attack determination model to train the attack determination model.

[110] The above description is based on the supervised binary classification model that
25 trains the attack determination model according to the model of the mobile terminal device and/or the user risk level. An unsupervised binary classification model may also be adopted to train the attack determination model based on sensor training data of different models of mobile terminal device and/or different user risk levels. Namely, in addition to using the sensor training data as input features, the risk level of the user corresponding to the sensor data
30 may also be used as an input feature, or the model of the mobile terminal device corresponding to the sensor data may also be used as an input feature, alternatively the risk level of the user and the mobile terminal device model corresponding to the sensor data may be both used as input features, or the like.

[111] An example of an attack determination model that supports various user risk levels

and/or different models of mobile terminal device is described above. In exemplary applications, one attack determination model may only correspond to one user risk level and/or one mobile terminal device model.

[112] It should be understood that, during the model training, the training may be performed based on sensor training data of different user risk levels and/or sensor data of different models of mobile terminal device to obtain attack determination models corresponding to different user risk levels and/or different models of mobile terminal device. For example, the training may be performed by using multiple sets of sensor training data of a mobile terminal device model A to obtain an attack determination model corresponding to the mobile terminal device model A, etc.

[113] Optionally, as an exemplary embodiment, there are multiple attack determination models, and each attack determination model corresponds to a different mobile terminal device model;

[114] where the step S120 may be, for example, implemented as follows:

[115] inputting the sensor training data into an attack determination model corresponding to the model of the mobile terminal device to determine whether an attack occurs.

[116] For example, with regard to a mobile terminal device of the model A, training may be performed based on sensor training data corresponding to the mobile terminal device of the model A to obtain an attack determination model corresponding to the mobile terminal device of the model A. With regard to a mobile terminal device of a model B, training may be performed based on sensor training data corresponding to the mobile terminal device of the model B to obtain an attack determination model corresponding to the mobile terminal device of the model B. Accordingly, when attack determination is performed, for the mobile terminal device of the model A, obtained sensor data (or processed sensor data) may be input into the attack determination model corresponding to the mobile terminal device of the model A, so as to obtain an attack determination result; for the mobile terminal device of the model B, obtained sensor data (or processed sensor data) may be input into the attack determination model corresponding to the mobile terminal device of the model B, so as to obtain an attack determination result, and the like.

[117] Optionally, as an exemplary embodiment, an attack determination model has different determination thresholds, and the determination thresholds are set based on risk levels of users corresponding to mobile terminal devices.

[118] For example, it is assumed again that user risk levels are divided into three types, i.e., low risk users, regular risk users, and high risk users. With regard to users of different risk

levels, different determination thresholds may be set for an attack determination model. For example, in an exemplary application, the determination threshold may be set at 60% for a low risk user; the determination threshold may be set at 50% for a regular risk user; and the determination threshold may be set at 40% for a high risk user. Assuming that the attack probability of a set of sensor data is determined by the attack determination model to be 45%, if this user's risk level is a low risk level, then the determined attack determination result is that no attack occurs since 45% is lower than the determination threshold of 60% corresponding to the low risk level; if this user's risk level is a regular risk level, then the determined attack determination result is that no attack occurs since 45% is lower than the determination threshold of 50% corresponding to the low risk level; and if this user's risk level is a high risk level, then the determined attack determination result is that an attack occurs since 45% is higher than the determination threshold of 40% corresponding to the low risk level. Therefore, for the same sensor data, the determination results may be different since users have different risk levels.

[119] It should be understood that an output result of an attack determination model may further be fed back to a system that performs biometric authentication and identification, so as to adjust the process of biometric authentication and identification.

[120] Furthermore, after the step S120, the method may further comprise:

[121] adjusting, based on an output result of the attack determination model, a security authentication level of the biometric authentication and identification;

[122] where the higher the probability of attack occurrence is indicated by the output result, the higher the security authentication level of the biometric authentication and identification becomes after the adjustment.

[123] Taking face recognition as an example, multiple sets of liveness detection steps may be prepared in a face recognition system based on facial expression and speech interaction for different security authentication levels. If the output risk level of the attack determination model exceeds a first designated threshold, a liveness detection step with a high security authentication level is output to perform authentication and identification on the user to prevent risks. If the output risk level of the attack determination model is lower than a second designated threshold, a liveness detection step with a low security authentication level is output to perform authentication and identification on the user to improve user experience. For example, in combination with Table 1, assuming that the output result of the attack determination model indicates that the risk level of risk occurrence is ultra-high risk, the security authentication level of the biometric authentication and identification is then adjusted

to the highest security authentication level corresponding to the “ultra-high risk,” etc.

[124] The solution of the embodiments of the present application will be further described below with reference to an exemplary embodiment.

[125] FIG. 3 is a schematic flow chart of training and prediction of biometric authentication and identification according to some embodiments of the present application. Here,

[126] the training phase may comprise historical data collection, data pre-processing, feature extraction, and binary classification model training. The prediction phase may comprise online data collection, data pre-processing, feature extraction, determination of whether an attack occurs based on a binary classification model, and the like, as well as output of a determination result to a biometric authentication and identification system. The binary classification model according to some embodiments of the present application is the attack determination model in the embodiment as shown in FIG. 1. For example, the flow chart shown in FIG. 3 may comprise the following.

[127] (1) Historical data collection

[128] A mobile terminal device collects sensor data obtained in a historical process of biometric authentication and identification. The sensor data may comprise the acceleration sensor data and/or the gyroscope data.

[129] For example, the mobile terminal device may obtain sensor data in the entire process of biometric authentication and identification or in a predetermined time period in the process of biometric authentication and identification. The sensor data may comprise sensor data of one or more dimensions in the 6 dimensions as shown in FIG. 2 and time stamp information corresponding to the sensor data.

[130] (2) Data pre-processing

[131] After the collection of the sensor data is completed, pre-processing operations, such as filtering operation, boundary detection operation, and length normalization operation, may be further performed on the sensor data, so as to eliminate noises due to shaky hands or inherent to the sensors themselves during collection, thereby obtaining sensor data with relatively high confidence. See relevant description of the embodiment as shown in FIG. 1 for exemplary implementations of filtering operation, boundary detection operation, and length normalization operation, which will not be elaborated.

[132] (3) Feature extraction

[133] Feature extraction is performed based on the sensor data obtained in the step (1) or based on the pre-processed sensor data in the step (2) to obtain sensor data with features extracted.

[134] For example, based on data of an acceleration sensor in three directions of x, y, and z axes in the entire or a predetermined time length in the process of biometric authentication and identification, feature data of the acceleration sensor in three directions of x, y, and z axes, such as an average, a standard deviation, a median, a maximum, a minimum, and an integral, may be obtained. Based on data of a gyroscope in three directions of x, y, and z axes in the entire or a predetermined time length in the process of biometric authentication and identification, feature data of the gyroscope in three directions of x, y, and z axes, such as an average, a standard deviation, a median, a maximum, a minimum, and an integral, may be obtained.

[135] It should be understood that the feature data such as the time length of performing the biometric authentication and identification may also be determined based on the data obtained by the acceleration sensor or the gyroscope.

[136] It should be understood that the sensor data with features extracted may comprise one or more pieces of the above-described feature data.

[137] (4) Binary classification model training

[138] During the model training, the sensor data obtained in the step (1) may be used as training data, the sensor data obtained after the pre-processing in the step (2) may be used as training data, or the sensor data obtained after the feature extraction in the step (3) may be used as training data.

[139] Apparently, when the sensor data obtained after the feature extraction in the step (3) is input as training data into the attack determination model, the trained attack determination model may be more accurate.

[140] With regard to the training of the attack determination model, supervised binary classification model training or unsupervised binary classification model training may be adopted, so that two types of application scenarios, i.e., with attack occurrence and without attack occurrence, are identified based on the sensor data. For an exemplary training method, the relevant model training methods in the current technologies may be referenced, which will not be elaborated.

[141] Moreover, it should be understood that, during the training of the attack determination model, the model of the mobile terminal device and/or the user risk level corresponding to the sensor data may be further used as an input feature of the attack determination model, or different attack determination models may be trained based on different models of mobile terminal device and/or different user risk levels.

[142] (5) Online data collection

[143] The step (1) may be referenced for an exemplary implementation of the step (5).

[144] (6) Data pre-processing

[145] The step (2) may be referenced for an exemplary implementation of the step (6).

[146] (7) Feature extraction

5 [147] The step (3) may be referenced for an exemplary implementation of the step (7).

[148] (8) Determination of whether an attack occurs based on a binary classification model.

[149] In this step, the sensor data obtained after the feature extraction may be used as an input to the binary classification model for determining whether an attack occurs.

[150] It should be understood that, if the binary classification model is trained based on
10 directly collected sensor data or is trained based on pre-processed sensor data, corresponding online data is used as an input to the binary classification model.

[151] Furthermore, if the binary classification model further uses the user risk level and/or the model of the mobile terminal device as an input for training, corresponding information of the user risk level and/or the model of the mobile terminal device also needs to be input when
15 determination is performed based on the binary classification model.

[152] If multiple binary classification models exist and each binary classification model corresponds to a user risk level and/or a model of mobile terminal device, a binary classification model corresponding to the user risk level and/or the model of mobile terminal device corresponding to the sensor data is selected for determination of the sensor data.

20 [153] (9) Output of a determination result to a biometric authentication and identification system.

[154] A determination result may be obtained based on the binary classification model.

[155] At this point, the determination result may be fed back to the biometric authentication and identification system, so that the biometric authentication and identification system
25 executes a corresponding operation.

[156] Optionally, the determination result may be fed back to the biometric authentication and identification system, so that the biometric authentication and identification system determines whether an attack occurs, thereby determining whether the current biometric authentication and identification is valid.

30 [157] Optionally, the determination result may be fed back to the biometric authentication and identification system, so that the biometric authentication and identification system determines whether to adjust the security level of the biometric authentication and identification, so as to take both security and user experience into consideration. For example, the determination result may be a risk level of the current biometric authentication and

identification, and based on this risk level and the current security level of the biometric authentication and identification, the biometric authentication and identification system may determine whether to adjust the security level of the biometric authentication and identification.

5 [158] For example, it is assumed that there are four risk levels in determination results, i.e., low risk, regular risk, high risk, and ultra-high risk, and that corresponding security levels of biometric authentication and identification are divided into Level 1, Level 2, Level 3, and Level 4, respectively (the higher the level is, the higher the authentication requirements are for the biometric authentication and identification, and generally speaking, the poorer the user
10 experience becomes). Assuming that the determination result is high risk and the security level of biometric authentication and identification is Level 1, then the biometric authentication and identification system may adjust the security level of biometric authentication and identification to Level 3. Assuming that the determination result is low risk and the security level of biometric authentication and identification is Level 4, then the biometric
15 authentication and identification system may adjust the security level of biometric authentication and identification to Level 1, and the like.

[159] Particular embodiments of the present specification are described above, and other embodiments fall within the scope of the appended claims. In certain situations, actions or steps stated in the claims may be executed in an order different from those in the embodiments
20 and can still achieve desired results. In addition, a process depicted in the accompanying drawings does not necessarily require the illustrated particular order or continuous order to achieve desired results. In some implementations, multi-task processing and parallel processing may be feasible or may be beneficial.

[160] FIG. 4 is a schematic structure diagram of an electronic device according to some
25 embodiments of the present application. Referring to FIG. 4, at a hardware level, the electronic device comprises a processor, and optionally may further comprise an internal bus, a network interface, and a memory, where the memory may comprise an internal memory, such as a Random-Access Memory (RAM), and may further comprise a non-volatile memory, such as at least one disk memory. The electronic device may also comprise hardware required by other
30 business.

[161] The processor, the network interface, and the memory may be connected to each other via the internal bus. The internal bus may be an Industry Standard Architecture (ISA) bus, a Peripheral Component Interconnect (PCI) bus, or an Extended Industry Standard Architecture (EISA) bus. The bus may be divided into an address bus, a data bus, a control bus, and the like.

For convenience of description, only one two-way arrow is used in FIG. 4 to represent the bus, which does not indicate that there is only one bus or one type of buses.

[162] The memory is used for storing programs. For example, the programs may comprise program codes, and the program codes comprise computer operation instructions. The memory
5 may comprise an internal memory and a non-volatile memory, and may provide instructions and data to the processor.

[163] The processor reads corresponding computer programs from the non-volatile memory into the internal memory, and then executes the computer programs to form a biometric authentication, identification, and detection apparatus on the logical level. The processor
10 executes programs stored in the memory and is configured, for example, to execute the following operations:

[164] obtaining sensor data of the mobile terminal device when the mobile terminal device performs biometric authentication and identification; and

[165] determining whether an attack occurs based on the sensor data and an attack
15 determination model;

[166] where the attack determination model is obtained based on training with sensor training data.

[167] The method implemented by the biometric authentication, identification, and detection device disclosed by the embodiment as shown in FIG. 1 of the present application
20 may be applied to a process or may be implemented by the processor. The processor may be an integrated circuit chip with signal processing capabilities. In an implementation process, the steps of the above-described method may be carried out by an integrated logic circuit of the hardware or instructions in the form of software in the processor. The above-described processor may be a general-purpose processor, including a Central Processing Unit (CPU), a
25 Network Processor (NP), a Digital Signal Processor (DSP), an Application Specific Integrated Circuit (ASIC), a Field-Programmable Gate Array (FPGA), or other programmable logic devices, discrete gates or transistor logic devices, and discrete hardware components, which can implement or execute the methods, steps, and logic block diagrams disclosed in the embodiments of the present application. The general-purpose processor may be a
30 micro-processor, or the processor may also be any conventional processor. Steps of the method disclosed with reference to the embodiments of the present application may be directly executed and completed by a hardware decoding processor or executed and completed by a combination of hardware and software modules in a decoding processor. The software modules may be disposed in a storage medium mature in the art, such as a random memory, a

flash memory, a read-only memory, a programmable read-only memory or an electrically erasable programmable memory, a register and the like. The storage medium is disposed in the memory, and the processor reads information in the memory and completes the steps of the above-described methods in combination with the hardware thereof.

5 [168] The electronic device may further implement the methods shown in FIG. 1 and achieve functions of the biometric authentication, identification, and detection apparatus in the embodiments as shown in FIG. 1, or achieve functions of the training phase and/or the prediction phase in the embodiments as shown in FIG. 2, which will not be elaborated by the embodiments of the present application.

10 [169] In addition to the software implementation, the electronic device according to the present application does not exclude other implementations, such as logic devices or a combination of software and hardware. In other words, the execution entities of the following processing flow are not limited to various logic units, but may also be hardware or logic devices.

15 [170] The embodiments of the present application further provide a computer readable storage medium, where the computer readable storage medium stores one or more programs, and the one or more programs comprise instructions can, when executed by a portable electronic device comprising a plurality of applications, cause the portable electronic device to implement the method in the embodiment as shown in FIG. 1, and to implement, for example,
20 the following operations:

[171] obtaining sensor data of the mobile terminal device when the mobile terminal device performs biometric authentication and identification; and

[172] determining whether an attack occurs based on the sensor data and an attack determination model;

25 [173] where the attack determination model is obtained based on training with sensor training data.

[174] FIG. 5 is a schematic structural diagram of a biometric authentication, identification, and detection apparatus 500 according to some embodiments of the present application. Referring to FIG. 5, in a software implementation, the biometric authentication, identification,
30 and detection apparatus 500 may comprise:

[175] an obtaining unit 501 configured to obtain sensor data of a mobile terminal device when the mobile terminal device performs biometric authentication and identification; and

[176] an attack determining unit 502 configured to determine whether an attack occurs based on the sensor data and an attack determination model;

[177] where the attack determination model is obtained based on training with sensor training data.

[178] In the embodiments of the present application, sensor data collected by a mobile terminal device during biometric authentication and identification is obtained, and attack determination is performed on the sensor data based on a sensor classification model. As a result, with reduced dependence or without dependence on user cooperation, the effect of strengthening the security of biometric authentication and identification can be achieved. The embodiments of the present application provide better security support for users while enhancing user experience.

[179] Optionally, as an exemplary embodiment, the obtaining unit 501 is further configured to obtain a risk level of a user corresponding to the mobile terminal device and/or model data of the mobile terminal device; and

[180] the attack determining unit 502 is further configured to:

[181] determine whether an attack occurs based on the risk level of a user corresponding to the mobile terminal device and/or the model data of the mobile terminal device, the sensor data and the attack determination model;

[182] where the training of the attack determination model uses sensor training data under the risk level of a user corresponding to the mobile terminal device and/or a model of the mobile terminal device.

[183] Alternatively, as another exemplary embodiment, there are optionally multiple attack determination models, and each attack determination model corresponds to a different mobile terminal device model;

[184] the attack determining unit 502 is configured, for example, to

[185] determine whether an attack occurs based on the sensor data and the attack determination model corresponding to the model of the mobile terminal device.

[186] Furthermore, an attack determination model has different determination thresholds, and the determination thresholds are set based on risk levels of users corresponding to mobile terminal devices.

[187] Alternatively, as another exemplary embodiment, an attack determination model optionally has different determination thresholds, and the determination thresholds are set based on risk levels of users corresponding to mobile terminal devices.

[188] Optionally, as an exemplary embodiment, the attack determining unit 502 is configured, for example, to

[189] pre-process the sensor data to obtain pre-processed sensor data, where the

pre-processing comprises at least one of the following: filtering operation, boundary detection operation, and length normalization operation; and

[190] determine whether an attack occurs based on the pre-processed sensor data and the attack determination model;

5 [191] where the attack determination model is obtained based on training with the pre-processed sensor training data.

[192] Optionally, as an exemplary embodiment, the attack determining unit 502 is configured, for example, to

10 [193] perform feature extraction on the sensor data to obtain the sensor data with features extracted; and

[194] determine whether an attack occurs based on the sensor data with features extracted and the attack determination model;

[195] where the attack determination model is obtained based on training with sensor training data with features extracted;

15 [196] the sensor data with features extracted comprises acceleration sensor data of the mobile terminal device and/or the gyroscope data of the mobile terminal device;

[197] the acceleration sensor data comprises one or more pieces of the following data: an average, a standard deviation, a median, a maximum, a minimum, and an integral of the acceleration sensor of the mobile terminal device in three directions of x, y, and z axes; and

20 [198] the gyroscope data comprises one or more pieces of the following data:

[199] an average, a standard deviation, a median, a maximum, a minimum, and an integral of the gyroscope of the mobile terminal device in three directions of x, y, and z axes.

[200] Furthermore, the sensor data with features extracted also comprises a time length of performing the biometric authentication and identification.

25 [201] For example, the sensor data subject to feature extraction may be the pre-processed sensor data or may be the sensor data that is not pre-processed.

[202] Optionally, the biometric authentication, identification, and detection apparatus 500 may further comprise a training unit 503, where the training unit 503 may be configured, for example, to

30 [203] obtain sensor data of the mobile terminal device collected when the mobile terminal device performed biometric authentication and identification historically to obtain multiple sets of sensor training data of the mobile terminal device; and

[204] use the multiple sets of sensor training data as inputs to the attack determination model for training to obtain the attack determination model.

[205] Furthermore, the training unit 503 may be configured, for example, to

[206] obtain sensor data of the mobile terminal device collected when the mobile terminal device performed biometric authentication and identification historically;

[207] determine sensor training data and a corresponding label based on the sensor data and corresponding attack occurrence situation, the label used for indicating whether an attack has occurred to the corresponding sensor training data; and

[208] use multiple sets of sensor training data and corresponding identifiers as inputs to the attack determination model for training to obtain the attack determination model.

[209] Furthermore, the training unit 503 may be configured, for example, to

[210] obtain sensor data of the mobile terminal device collected when the mobile terminal device performed biometric authentication and identification historically;

[211] determine sensor training data based on the sensor data; and

[212] use multiple sets of sensor training data as inputs to the attack determination model for performing clustering training on the multiple sets of historical sensor data to obtain the attack determination model.

[213] Optionally, the biometric authentication, identification, and detection apparatus 500 may further comprise an adjusting unit 504, where the adjusting unit 504 may be configured, for example, to

[214] adjust, based on an output result of the attack determination model, a security authentication level of the biometric authentication and identification;

[215] where the higher the probability of attack occurrence is indicated by the output result, the higher the security authentication level of the biometric authentication and identification becomes after the adjustment.

[216] In summary, the above-described is merely preferred embodiments of the present application, which are not used to limit the scope of the present application. Any modification, equivalent substitution, or improvement made within the spirit and principle of the present application shall fall within the scope of the present application.

[217] The system, device, module, or unit elaborated in the above-described embodiments may be achieved, for example, by a computer chip or entity or by a product having a function.

One typical implementation apparatus is a computer. For example, the computer may be a personal computer, a laptop computer, a cellular telephone, a camera phone, a smart phone, a personal digital assistant, a media player, a navigation device, an email device, a game console, a tablet computer, a wearable device, or a combination of any of the above apparatuses.

[218] Computer readable media include non-volatile, volatile, mobile, and immobile media,

which can implement information storage through any method or technology. The information may be computer readable instructions, data structures, program modules, or other data. Examples of storage media of computers include, but are not limited to, Phase-change Random Access Memories (PRAMs), Static Random Access Memories (SRAMs), Dynamic Random Access Memories (DRAMs), other types of Random Access Memories (RAMs), Read-Only Memories (ROMs), Electrically Erasable Programmable Read-Only Memories (EEPROMs), flash memories or other memory technologies, Compact Disk Read-Only Memories (CD-ROMs), Digital Versatile Discs (DVDs) or other optical memories, magnetic cassettes, magnetic cassette and disk memories or other magnetic storage devices, or any other non-transmission media, which can be used for storing information accessible to a computation device. According to the description in the present specification, the computer readable media do not include transitory media, such as modulated data signals and carriers.

[219] It should be further noted that the terms of “including,” “comprising,” or any other variants of the terms are intended to encompass a non-exclusive inclusion, causing a process, method, product, or device comprising a series of elements to not only comprise these elements, but also comprise other elements that are not explicitly listed, or further comprise elements that are inherent to the process, method, product, or device. When there is no further restriction, elements described by the statement “comprising one...” does not exclude that a process, method, product, or device comprising the above elements further comprises additional identical elements.

[220] The various embodiments in the present specification are described in a progressive manner, the same or similar parts between the various embodiments may refer to each other, and each embodiment focuses on the difference from the other embodiments. In particular, since the system embodiments are substantially similar to the method embodiments, the system embodiments are described in a relatively simple manner, and the description of relevant parts of the method embodiments may be referenced.

Claims

1. A biometric authentication, identification, and detection method for a mobile terminal device, comprising:

5 obtaining sensor data of the mobile terminal device when the mobile terminal device performs biometric authentication and identification; and

determining whether an attack occurs based on the sensor data and an attack determination model;

10 wherein the attack determination model is obtained based on training with sensor training data.

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

obtaining a risk level of a user corresponding to the mobile terminal device and/or model data of the mobile terminal device; wherein

15 the determining whether an attack occurs based on the sensor data and an attack determination model comprises:

determining whether an attack occurs based on the risk level of a user corresponding to the mobile terminal device and/or model data of the mobile terminal device, the sensor data and the attack determination model;

20 wherein the training of the attack determination model is trained by using sensor training data under the risk level of the user corresponding to the mobile terminal device and/or a model of the mobile terminal device.

25 3. The method according to claim 1, wherein there are multiple attack determination models, and each attack determination model corresponds to a different mobile terminal device model; and

the determining whether an attack occurs based on the sensor data and an attack determination model comprises:

30 determining whether an attack occurs based on the sensor data and the attack determination model corresponding to a model of the mobile terminal device.

4. The method according to claim 1 or 3, wherein the attack determination model has different determination thresholds, and the determination thresholds are set based on risk levels of users corresponding to mobile terminal devices.

5. The method according to claim 1, wherein

the determining whether an attack occurs based on the sensor data and an attack determination model comprises:

5 pre-processing the sensor data to obtain pre-processed sensor data, the pre-processing comprising at least one of the following: filtering operation, boundary detection operation, and length normalization operation; and

determining whether an attack occurs based on the pre-processed sensor data and the attack determination model;

10 wherein the attack determination model is obtained based on training with the pre-processed sensor training data.

6. The method according to claim 1 or 5, wherein

15 the determining whether an attack occurs based on the sensor data and an attack determination model comprises:

performing feature extraction based on the sensor data to obtain the sensor data with features extracted; and

determining whether an attack occurs based on the sensor data with features extracted and the attack determination model;

20 wherein the attack determination model is obtained based on training with sensor training data with features extracted;

the sensor data with features extracted comprises acceleration sensor data of the mobile terminal device and/or gyroscope data of the mobile terminal device;

25 the acceleration sensor data comprises one or more pieces of the following data: an average, a standard deviation, a median, a maximum, a minimum, and an integral of an acceleration sensor of the mobile terminal device in three directions of x, y, and z axes; and

the gyroscope data comprises one or more pieces of the following data:

an average, a standard deviation, a median, a maximum, a minimum, and an integral of a gyroscope of the mobile terminal device in three directions of x, y, and z axes.

30

7. The method according to claim 6, wherein the sensor data with features extracted also comprises a time length of performing the biometric authentication and identification.

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

adjusting, based on an output result of the attack determination model, a security authentication level of the biometric authentication and identification;

wherein the higher a probability of attack occurrence is indicated by the output result, the higher the security authentication level of the biometric authentication and identification becomes after the adjustment.

9. A biometric authentication, identification, and detection apparatus, comprising:

an obtaining unit configured to obtain sensor data of a mobile terminal device when the mobile terminal device performs biometric authentication and identification; and

an attack determining unit configured to determine whether an attack occurs based on the sensor data and an attack determination model;

wherein the attack determination model is obtained based on training with sensor training data.

10. An electronic device, comprising:

a processor; and

a memory configured to store computer executable instructions, wherein the executable instructions cause, when executed, the processor to execute the following operations:

obtaining sensor data of a mobile terminal device when the mobile terminal device performs biometric authentication and identification; and

determining whether an attack occurs based on the sensor data and an attack determination model;

wherein the attack determination model is obtained based on training with sensor training data.

11. A computer readable storage medium, wherein the computer readable storage medium stores one or more programs, and the one or more programs, when executed by an electronic device comprising a plurality of applications, cause the electronic device to execute the following operations:

obtaining sensor data of a mobile terminal device when the mobile terminal device performs biometric authentication and identification; and

determining whether an attack occurs based on the sensor data and an attack determination model;

wherein the attack determination model is obtained based on training with sensor

training data.