Claims

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

obtaining a risk level of a user corresponding to the mobile terminal device;

determining a time length for collecting sensor data of the mobile terminal device based on the obtained risk level of the user, wherein the time length for collecting the sensor data of the mobile terminal device is increased with an increased risk level of the user;

obtaining the sensor data of the mobile terminal device for the determined time length, wherein the sensor data is collected when the mobile terminal device performs biometric authentication and identification; and

determining whether an attack occurs in the biometric authentication by inputting the sensor data and the risk level of the user into an attack determination model;

wherein the attack determination model is trained by using the risk level of the user and sensor training data obtained based on sensor data of the mobile terminal device collected when the mobile terminal device performed biometric authentication historically.

2. 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 in the biometric authentication comprises:

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

3. The method according to claim 1 or 2, 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.

4. The method according to claim 1, wherein

the determining whether an attack occurs in the biometric authentication comprises:

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

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

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

5. The method according to claim 1 or 4, wherein

the determining whether an attack occurs in the biometric authentication 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;

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;

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.

6. 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.

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

an obtaining unit configured to

obtain a risk level of a user corresponding to a mobile terminal device;

determine a time length for collecting sensor data of the mobile terminal device based on the obtained risk level of the user, wherein the time length for collecting the sensor data of the mobile terminal device is increased with an increased risk level of the user; and

obtain the sensor data of the mobile terminal device for the determined time length, wherein the sensor data is collected when the mobile terminal device performs biometric authentication and identification; and

an attack determining unit configured to determine whether an attack occurs in the biometric authentication by inputting the sensor data and the risk level of the user into an attack determination model;

wherein the attack determination model is trained by using the risk level of the user and sensor training data obtained based on sensor data of the mobile terminal device collected when the mobile terminal device performed biometric authentication historically.

8. 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 a risk level of a user corresponding to a mobile terminal device;

determining a time length for collecting sensor data of the mobile terminal device based on the obtained risk level of the user, wherein the time length for collecting sensor data of the mobile terminal device is increased with an increased risk level of the user;

obtaining the sensor data of the mobile terminal device for the determined time length, wherein the sensor data is collected when the mobile terminal device performs biometric authentication and identification; and

determining whether an attack occurs in the biometric authentication by inputting the sensor data and the risk level of the user into an attack determination model;

wherein the attack determination model is trained by using the risk level of the user and sensor training data obtained based on sensor data of the mobile terminal device collected when the mobile terminal device performed biometric authentication historically.

9. 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 a risk level of a user corresponding to the mobile terminal device;

determining a time length for collecting sensor data of the mobile terminal device based on the obtained risk level of the user, wherein the time length for collecting sensor data of the

mobile terminal device is increased with an increased risk level of the user;

obtaining sensor data of the mobile terminal device for the determined time length, wherein the sensor data is collected when the mobile terminal device performs biometric authentication and identification; and

determining whether an attack occurs in the biometric authentication by inputting the sensor data and the risk level of the user into an attack determination model;

wherein the attack determination model is trained by using the risk level of the user and sensor training data obtained based on sensor data of the mobile terminal device collected when the mobile terminal device performed biometric authentication historically.