

Claims

1. A method for identity authentication, comprising:
 - collecting, by a terminal, each time a user performs a specified operation on the terminal, action attribute information with respect to each of multiple processes in performing the specified operation, as sample information;
 - determining an action attribute value range according to the sample information, with respect to each of the multiple processes;
 - presetting the action attribute value range as standard information, with respect to each of the multiple processes,
 - collecting, by the terminal, target action attribute information of a target user in performing the multiple processes of the specified operation-when the target user performs the specified operation;
 - determining, according to the preset standard information, whether the target action attribution information is matched with the standard information, with respect to each of the multiple processes;
 - if yes, determining that the authentication is successful, and performing corresponding processing according to the specified operation; and
 - otherwise, determining that the authentication is failed, and refusing to perform the corresponding processing according to the specified operation,
 - wherein the determining an action attribute value range according to the sample information specifically comprises, with respect to each of the multiple processes:
 - determining a first average value of each sample information according to each sample information;
 - determining a second average value of sample information greater than the first average value;
 - determining a third average value of sample information not greater than the first average value; and
 - determining a numerical range from the third average value to the second average value as the action attribute value range,

wherein the sample information includes tap strength value of a tap action on a touch screen of the terminal or acceleration information of the terminal when the user raises the terminal.

2. The method according to claim 1, wherein the determining whether the target action attribution information is matched with the standard information specifically comprises:

determining whether an attribute value included in the target action attribute information falls within the action attribute value range, with respect to each of the multiple processes;

if yes, determining that the target action attribute information is matched with the standard information; and

otherwise, determining that the target action attribution information is not matched with the standard information.

3. The method according to any of claims 1 and 2, wherein the action attribute information comprises one or more of applied force information and acceleration information.

4. A device for identity authentication, comprising: a collection module, a determination module, and a processing module, wherein

the collection module is configured to:

collect, each time a user performs a specified operation, action attribute information with respect to each of multiple processes in performing the specified operation, as sample information; and

collect target action attribute information of a target user in performing the multiple processes of the specified operation when the target user performs the specified operation;

the determination module is configured to:

determine an action attribute value range according to the sample information with respect to each of the multiple processes;

preset the action attribute value range as standard information with respect to each of the multiple processes,

determine, according to the standard information, whether the target action attribution information is matched with the standard information, with respect to each of the multiple processes; and

the processing module is configured to: when the determination module determines that there is a matching, determine that the authentication is successful, and perform corresponding processing according to the specified operation; and when the determination module determines that there is no matching, determine that the authentication is failed, and refuse to perform the corresponding processing according to the specified operation,

wherein the determination module is specifically configured to, with respect to each of the multiple processes:

determine a first average value of each sample information according to each sample information; determine a second average value of sample information greater than the first average value; determine a third average value of sample information not greater than the first average value; and determine a numerical range from the third average value to the second average value as the action attribute value range,

wherein the sample information includes tap strength value of a tap action on a touch screen of the device or acceleration information of the device when the user raises the device.

5. The device according to claim 4, wherein the determination module is specifically configured to:

determine whether an attribute value included in the target action attribute information falls within the action attribute value range, with respect to each of the multiple processes; if yes, determine that the target action attribute information is matched with the standard information; otherwise, determine that the target action attribute information is not matched with the standard information.

6. The device according to any of claims 4 and 5, wherein the action attribute information comprises one or more of applied force information and acceleration information.