

CLAIMS

1. A method for user identity verification, the method comprising:

collecting interaction behavior characteristics of a user wearing a virtual reality terminal by using preset sensing hardware in response to an execution instruction for a target task requiring identity verification;

matching the collected interaction behavior characteristics with preset interaction behavior characteristics of a legal user of the virtual reality terminal to verify an identity of the user, wherein matching comprises:

obtaining a preset behavioral interaction characteristic identification model representing the behavioral interaction characteristics of the user wearing the virtual reality terminal, wherein the preset interaction behavior characteristic identification model is obtained by training with several interaction behavior characteristic samples of the legal user of the virtual reality terminal based on a preset deep learning algorithm, and

comparing the obtained additional interaction characteristics of the user with the preset behavioral interaction characteristic identification model to determine whether the collected interaction behavior characteristics match habitual interaction behavior characteristics of the legal user of the virtual reality terminal;

determining that the user wearing the virtual reality terminal has a legal identity; and

executing the target task if the collected interaction behavior characteristics match the preset interaction behavior characteristics.

2. The method of claim 1, wherein the interaction behavior characteristics comprise any one of a head posture of the user, a three-dimensional gesture, and a displacement track generated by movement of a visual focus controlled through the head posture, the three-dimensional gesture, or an external device.

3. The method of claim 1, further comprising:

executing further security authentication for the user when a number of identity verifications for the user wearing the virtual reality terminal reaches a preset number of times, if the collected interaction behavior characteristics do not match the preset interaction behavior

characteristics; and

determining that the user wearing the virtual reality terminal has a legal identity and executing the target task after the security authentication is successful.

4. The method of claim 1, further comprising:

collecting the interaction behavior characteristics of the user wearing the virtual reality terminal by using the preset sensing hardware after it is determined that the user wearing the virtual reality terminal has a legal identity; and

inputting the collected interaction behavior characteristics into the preset interaction behavior characteristic identification model.

5. The method of claim 1, wherein the preset deep learning algorithm comprises a deep learning algorithm such as a neural network and a regression algorithm.

6. The method of claim 1, wherein the preset interaction behavior characteristic identification model represents the habitual interaction behavior characteristics of the legal user of the virtual reality terminal.

7. The method of claim 1, further comprising:

executing further security authentication for the user wearing the virtual reality terminal if the collected interaction behavior characteristics do not match the habitual interaction behavior characteristics of the legal user of the virtual reality terminal.

8. The method of claim 7, wherein the step of executing further security authentication for the user comprises:

collecting biometric characteristics of the user by using preset biological identification hardware;

matching the collected biometric characteristics with preset biometric characteristics of the legal user of the virtual reality terminal; and

determining that the security authentication for the user is successful if the collected

biometric characteristics match the preset biometric characteristics of the legal user of the virtual reality terminal.

9. The method of claim 7, wherein the step of executing further security authentication for the user comprises:

acquiring an identity verification password input by the user;

matching the acquired identity verification password with a preset identity verification password; and

determining that the security authentication for the user is successful if the acquired identity verification password matches the preset identity verification password of the legal user of the virtual reality terminal.

10. The method of claim 1, wherein the target task comprises a task for unlocking the virtual reality terminal.

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