

CLAIMS

What is claimed is:

1. An identity recognition method, used to: based on one or more touch-enabled devices and one or more monitoring devices that are on a real-world user side,
5 recognize an identity of a first user from multiple users on the user side by using an identity recognition model on a server side; and the method comprises:

recognizing a touching on the touch-enabled device, and obtaining video streams of the multiple users that are recorded by the monitoring device, wherein recognizing the touching on the touch-enabled device comprises:

10 monitoring, by the monitoring device, a behavior that a user performs a touching on the touch-enabled device, and

uploading, to the identity recognition model, a video stream that comprises a performing behavior of the touching;

locking, based on the video streams, ~~a~~the user who performs the touching as the
15 first user, and obtaining biometric features of the first user; and

recognizing the identity of the first user based on the biometric features of the first user.

2. The method according to claim 1, wherein recognizing a touching on the touch-enabled device comprises:

20 after the user performs the touching on the touch-enabled device, reporting, by the touch-enabled device, the touching to the identity recognition model.

3. The method according to claim 2, wherein locking, based on the video streams, a user who performs the touching as the first user comprises:

25 determining, by the identity recognition model, a timestamp of the touching based on the touching reported by the touch-enabled device; and

searching, by the identity recognition model, the video streams uploaded by the monitoring device for a video stream corresponding to the timestamp, and recognizing a user in the video stream corresponding to the timestamp as the first user.

30 ~~4. The method according to claim 1, wherein recognizing a touching on the touch-enabled device comprises:~~

~~monitoring, by the monitoring device, a behavior that the user performs a touching on the touch-enabled device, and uploading, to the identity recognition~~

~~model, a video stream that comprises a performing behavior of the touching.~~

54. The method according to claim 41, wherein locking, based on the video streams, a user who performs the touching as the first user comprises:

5 determining, by the identity recognition model based on image analysis on the video stream comprising the performing behavior of the touching, that the user who performs the touching is the first user.

65. The method according to claim 3 or 54, wherein obtaining biometric features of the first user based on the video streams of the multiple users that are recorded by the monitoring device comprises:

10 performing image analysis on a video stream corresponding to the first user, to obtain an image of the first user; and

performing biometric feature extraction based on the image of the first user, to obtain the biometric features of the first user.

76. The method according to any one of claims 1 to 65, wherein recognizing the identity of the first user based on the biometric features of the first user comprises:

15 comparing the obtained biometric features of the first user with prestored user identity features; and

if the biometric features of the first user are comprised in the prestored user identity features, determining that the first user is a prestored user.

20 87. The method according to claim 76, further comprising:

confirming an identity recognition result and communicating information about the identity recognition result.

98. The method according to any one of claims 1 to 65, wherein scenarios on the user side comprise: a facial recognition-based payment and/or iris scanning-based payment scenario, a facial recognition-based access and/or iris scanning-based access scenario, a facial recognition-based public transportation boarding scenario and/or iris scanning-based public transportation boarding scenario.

109. An identity recognition model, configured to: based on one or more touch-enabled devices and one or more monitoring devices that are on a real-world user side, recognize an identity of a first user from multiple users on the user side by using the identity recognition model on a server side; and the identity recognition model comprises:

a touching recognition unit, configured to recognize a touching on the touch-enabled device, wherein the touching recognition unit is specifically configured

to receive a video stream that comprises a performing behavior of the touching and that is uploaded by the monitoring device;

a video stream acquisition unit, configured to obtain video streams of the multiple users that are recorded by the monitoring device;

5 a user locking unit, configured to lock, based on the video streams, a user who performs the touching as the first user;

a user biometric feature acquisition unit, configured to obtain biometric features of the first user based on the video streams; and

10 an identity recognition unit, configured to recognize the identity of the first user based on the biometric features of the first user.

~~11~~10. The apparatus according to claim ~~10~~9, wherein the touching recognition unit is specifically configured to: after the user performs the touching on the touch-enabled device, receive the touching reported by the touch-enabled device.

15 ~~12~~11. The apparatus according to claim ~~11~~10, wherein the user locking unit is specifically configured to determine a timestamp of the touching based on the touching reported by the touch-enabled device; and search the video streams uploaded by the monitoring device for a video stream corresponding to the timestamp, and recognize a user in the video stream corresponding to the timestamp as the first user.

20 ~~13. The apparatus according to claim 10, wherein the touching recognition unit is specifically configured to receive a video stream that comprises a performing behavior of the touching and that is uploaded by the monitoring device.~~

~~14~~12. The apparatus according to claim ~~13~~9, wherein the user locking unit is specifically configured to: determine, based on image analysis on the video stream comprising the performing behavior of the touching, that the user who performs the touching is the first user.

~~15~~13. The apparatus according to claim ~~12-11~~ or ~~14~~12, wherein the user biometric feature acquisition unit is specifically configured to:

perform image analysis on a video stream corresponding to the first user, to obtain an image of the first user; and

30 perform biometric feature extraction based on the image of the first user, to obtain the biometric features of the first user.

~~16~~14. The apparatus according to any one of claims ~~10-9~~ to ~~15~~13, wherein the identity recognition unit is specifically configured to: compare the obtained biometric features of the first user with prestored user identity features; and if the biometric

features of the first user are comprised in the prestored user identity features, determine that the first user is a prestored user.

~~17~~15. The apparatus according to claim ~~16~~14, further comprising:

5 a recognition confirmation unit, configured to confirm an identity recognition result and communicate information about the identity recognition result.

~~18~~16. The apparatus according to any one of claims ~~10-9~~ to ~~15~~13, wherein scenarios on the user side comprise: a facial recognition-based payment and/or iris scanning-based payment scenario, a facial recognition-based access and/or iris scanning-based access scenario, a facial recognition-based public transportation
10 boarding scenario and/or iris scanning-based public transportation boarding scenario.

~~19~~17. An identity recognition system, comprising one or more touch-enabled devices, one or more monitoring devices, and an identity recognition model, and configured to recognize an identity of a first user from multiple users on a server side based on the touch-enabled device and the monitoring device that are on a real-world
15 user side, wherein

the touch-enabled device is touchable by a user, so as to record a touching;

the monitoring device is configured to (i) obtain video streams of the multiple users and upload the video streams to the identity recognition model, and (ii) monitor a behavior that the user performs the touching on the touch-enabled device, and
20 upload, to the identity recognition model, a video stream that comprises a performing behavior of the touching; and

the identity recognition model is configured to: recognize a touching on the touch-enabled device, lock, based on the video streams of the monitoring device, the first user that performs the touching, obtain user biometric features of the first user,
25 and perform identity recognition based on the user biometric features.

~~20~~18. The system according to claim ~~19~~17, wherein

the touch-enabled device is configured to obtain the touching of the user and report the touching to the identity recognition model; and

the identity recognition model is specifically configured to: after the user
30 performs the touching on the touch-enabled device, report, by the touch-enabled device, the touching to the identity recognition model.

~~21~~19. The system according to claim ~~20~~18, wherein the identity recognition model is specifically configured to determine a timestamp of the touching based on the touching reported by the touch-enabled device; and search the video streams

uploaded by the monitoring device for a video stream corresponding to the timestamp, and recognize a user in the video stream corresponding to the timestamp as the first user.

~~22. The system according to claim 19, wherein the monitoring device is further~~
5 ~~configured to: monitor a behavior that the user performs the touching on the touch-enabled device, and upload, to the identity recognition model, a video stream that comprises a performing behavior of the touching.~~

~~23~~20. The system according to claim ~~22~~17, wherein the identity recognition model is further configured to: determine, based on image analysis on the video
10 stream comprising the performing behavior of the touching, that the user who performs the touching is the first user.

~~24~~21. The system according to claim ~~21-19~~ or ~~23~~20, wherein the identity recognition model is specifically configured to: perform image analysis on the video stream corresponding to the first user, to obtain an image of the first user; and perform
15 biometric feature extraction based on the image of the first user, to obtain the biometric features of the first user.

~~25~~22. The system according to any one of claims ~~19-17~~ to ~~24~~21, wherein the identity recognition model is specifically configured to: compare the obtained biometric features of the first user with prestored user identity features; and if the
20 biometric features of the first user are comprised in the prestored user identity features, determine that the first user is a prestored user.

~~26~~23. The system according to claim ~~25~~22, wherein the identity recognition model is further configured to: confirm an identity recognition result, and communicate information about the identity recognition result.

~~27~~24. The system according to any one of claims ~~19-17~~ to ~~24~~21, wherein scenarios on the user side comprise: a facial recognition-based payment and/or iris scanning-based payment scenario, a facial recognition-based access and/or iris scanning-based access scenario, a facial recognition-based public transportation boarding scenario and/or iris scanning-based public transportation boarding scenario.

~~28~~25. A server, comprising a memory, a processor, and a computer program that is stored in the memory and that can run on the processor, wherein when executing the program, the processor implements steps of the method according to any one of
30 claims 1 to ~~9~~8.

~~29~~26. A computer readable storage medium on which a computer program is

stored, wherein steps of the method according to any one of claims 1 to ~~9~~8 are implemented when the program is executed by a processor.