

FACIAL RECOGNITION METHODS AND APPARATUSES

ABSTRACT

Embodiments of the present specification provide a facial recognition method and apparatus. The method includes the following: An end-user device performs
5 homomorphic encryption on a to-be-recognized facial image by using a second public key to obtain an encrypted facial image, and transmits a recognition request including the encrypted facial image and the second public key to a server. The server performs homomorphic feature processing on the encrypted facial image and adds first obfuscation to the encrypted facial image in a homomorphic way, and adds second
10 obfuscation to pre-stored encrypted facial features in the homomorphic way. The end-user device receives obfuscated and encrypted output features and obfuscated and encrypted facial features from the server, decrypts the obfuscated and encrypted facial features by using a first private key corresponding to a first public key to obtain a first intermediate value, decrypts the obfuscated and encrypted output features by using a
15 second private key corresponding to the second public key to obtain a second intermediate value, calculates a difference between the second intermediate value and the first intermediate value, and transmits the difference to the server. The server determines whether the to-be-recognized facial image corresponds to a target user. The security and response speed of facial recognition can be improved.

20

FIG. 2