

WHAT IS CLAIMED IS:

1. A data processing method, comprising:

receiving target biometric information and verification password information of a target
5 object sent by an acquirer server;

determining partition biometric information from registered biometric information of a
plurality of objects, wherein the partition biometric information is registered biometric
information stored in association with the verification password information;

determining a main recognition algorithm and an auxiliary recognition algorithm
10 corresponding to the verification password information;

recognizing matched registered biometric information, matched with the target biometric
information, from the partition biometric information corresponding to the verification
password information through the main recognition algorithm;

verifying a recognition result of the main recognition algorithm through the auxiliary
15 recognition algorithm;

determining target account information of the target object according to the matched
registered biometric information, wherein registered biometric information of any of the objects
and registered account information of the any object are associatively stored; and

sending a data processing request to a card issuer server corresponding to the target account
20 information, wherein the data processing request comprises the target account information and
the verification password information, so that the card issuer server performs verification
through the verification password information and performs data processing according to the
target account information after the verification is passed.

25 2. The method according to claim 1, wherein the recognizing the matched registered biometric
information, matched with the target biometric information, from the partition biometric
information comprises:

comparing an information quantity of the partition biometric information with a quantity
threshold value;

30 recognizing the matched registered biometric information, matched with the target
biometric information, from the partition biometric information when the information quantity
is smaller than the quantity threshold value;

selecting out sub-partition biometric information from the partition biometric information through an algorithm when the information quantity is larger than or equal to the quantity threshold value, and recognizing the matched registered biometric information, matched with the target biometric information, from the sub-partition biometric information.

5

3. The method according to claim 2, further comprising:

sending a recognition failure response to a terminal through the acquirer server when it fails to recognize the matched registered biometric information matched with the target biometric information from the sub-partition biometric information, so that the terminal displays a prompt
10 of inputting auxiliary recognition information;

receiving the auxiliary recognition information forwarded by the acquirer server, wherein the auxiliary recognition information is sent by the terminal to the acquirer server in response to operation of a user;

determining registered biometric information corresponding to the auxiliary recognition
15 information from the sub-partition biometric information; and

recognizing the matched registered biometric information, matched with the target biometric information, from the registered biometric information corresponding to the auxiliary recognition information.

20 4. The method according to claim 1, wherein before sending the data processing request to the card issuer server corresponding to the target account information, the method further comprises:

sending the target account information to a terminal through the acquirer server, so that the terminal sends the data processing request to the acquirer server, wherein the data processing
25 request comprises the target account information and the verification password information; and

receiving the data processing request forwarded by the acquirer server.

5. The method according to claim 1, wherein before receiving the target biometric information and the verification password information of the target object, the method further comprises:

30 receiving registered account information, registered biometric information and routing index information of the target object, wherein the routing index information is generated by

operating the verification password information through an irreversible algorithm;

performing salt encryption processing on the routing index information; and

storing encrypted routing index information, the registered biometric information and the registered account information of the target object associatively.

5

6. The method according to claim 5, wherein the storing the encrypted routing index information, the registered biometric information and the registered account information of the target object associatively comprises:

10 performing tokenization processing on the registered account information of the target object so as to obtain Tokend information of the target object; and

storing the encrypted routing index information, the registered biometric information and the Tokend information of the target object associatively;

the determining the target account information of the target object, comprising:

determining Tokend information corresponding to the target biometric information; and

15 converting the Tokend information corresponding to the target biometric information into Tokent information; and

after determining the target account information of the target object, further comprising:

sending the Tokent information to a terminal.

20 7. The method according to any of claims 1 to 6, wherein the biometric information comprises one or more of:

face information, fingerprint information, vocal print information, iris information, palm print information, finger vein information or palm vein information.

25 8. A data processing apparatus, comprising:

a transceiving component, configured to receive target biometric information and verification password information of a target object sent by an acquirer server;

a recognition component, configured to:

30 determine partition biometric information from registered biometric information of a plurality of objects;

determine a main recognition algorithm and an auxiliary recognition algorithm corresponding to the verification password information;

recognize matched registered biometric information, matched with the target biometric information, from the partition biometric information corresponding to the verification password information through the main recognition algorithm; and

verify a recognition result of the main recognition algorithm through the auxiliary recognition algorithm; wherein the partition biometric information is registered biometric information stored in association with the verification password information; and

a determining component, configured to determine target account information of the target object according to the matched recognized registered biometric information, wherein registered biometric information of any of the objects and registered account information of the any object are associatively stored; wherein

the transceiving component is further configured to send a data processing request to a card issuer server corresponding to the target account information, wherein the data processing request comprises the target account information and the verification password information, so that the card issuer server performs verification through the verification password information and performs data processing according to the target account information after the verification is passed.

9. The apparatus according to claim 8, wherein the recognition component is configured to:

compare an information quantity of the partition biometric information with a quantity threshold value;

recognize the matched registered biometric information, matched with the target biometric information, from the partition biometric information when the information quantity is smaller than the quantity threshold value; and

select out sub-partition biometric information from the partition biometric information through an algorithm when the information quantity is larger than or equal to the quantity threshold value, and recognize the matched registered biometric information, matched with the target biometric information, from the sub-partition biometric information.

10. The apparatus according to claim 9, wherein

the transceiving component is further configured to send a recognition failure response to a

terminal through the acquirer server when it fails to recognize the matched registered biometric information matched with the target biometric information from the sub-partition biometric information, so that the terminal displays a prompt of inputting auxiliary recognition information; receive the auxiliary recognition information forwarded by the acquirer server,
5 wherein the auxiliary recognition information is sent by the terminal to the acquirer server in response to operation of a user; and

the recognition component is further configured to determine registered biometric information corresponding to the auxiliary recognition information from the sub-partition biometric information; and recognize the matched registered biometric information, matched
10 with the target biometric information, from the registered biometric information corresponding to the auxiliary recognition information.

11. The apparatus according to claim 8, wherein the transceiving component is further configured to:

15 send the target account information to a terminal through the acquirer server, so that the terminal sends the data processing request to the acquirer server, wherein the data processing request comprises the target account information and the verification password information; and
receive the data processing request forwarded by the acquirer server.

20 12. The apparatus according to claim 8, further comprising a registration component configured to:

receive registered account information, registered biometric information and routing index information of the target object, wherein the routing index information is generated by operating the verification password information through an irreversible algorithm;

25 perform salt encryption processing on the routing index information; and
store encrypted routing index information, the registered biometric information and the registered account information of the target object associatively.

13. The apparatus according to claim 12, wherein

30 the registration component is configured to perform tokenization processing on the registered account information of the target object so as to obtain Tokend information of the

target object; and store the encrypted routing index information, the registered biometric information and the Tokend information of the target object associatively;

the determining component is further configured to determine Tokend information corresponding to the target biometric information; and convert the Tokend information corresponding to the target biometric information into Token information; and

the transceiving component is further configured to send the Token information to a terminal.

14. The apparatus according to any of claims 8 to 13, wherein the biometric information comprises one or more of:

face information, fingerprint information, vocal print information, iris information, palm print information, finger vein information or palm vein information.

15. An electronic device, comprising:

at least one processor; and

a memory in communication connection with the at least one processor, wherein

the memory stores an instruction capable of being executed by the at least one processor, and the instruction is executed by the at least one processor to perform the method according to any of claims 1 to 7.

16. A non-transitory computer readable storage medium, storing a computer instruction, wherein the computer instruction is executed by a computer to perform the method according to any of claims 1 to 7.

17. A data processing system, comprising an acquirer server, a biometric recognition server and a card issuer server, wherein

the acquirer server is configured to receive target biometric information and verification password information of a target object sent by a terminal; and send the target biometric information and the verification password information to the biometric recognition server;

the biometric recognition server is configured to receive the target biometric information

and the verification password information sent by the acquirer server; determine partition biometric information from registered biometric information of a plurality of objects; determine a main recognition algorithm and an auxiliary recognition algorithm corresponding to the verification password information; recognize matched registered biometric information,
5 matched with the target biometric information, from the partition biometric information corresponding to the verification password information through the main recognition algorithm; and verify a recognition result of the main recognition algorithm through the auxiliary recognition algorithm; determine target account information of the target object according to the matched registered biometric information; and send a data processing request to the card issuer
10 server corresponding to the target account information, wherein the data processing request comprises the target account information and the verification password information; the partition biometric information is registered biometric information stored in association with the verification password information; and registered biometric information of any of the object and registered account information of the any object are stored associatively; and
15 the card issuer server is configured to receive the data processing request; and perform verification through the verification password information and perform data processing according to the target account information after the verification is passed.