

smaller than the quantity threshold value; and

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.

[0010] In an optional embodiment, the method further includes:

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 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 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.

[0011] In an optional embodiment, before sending the data processing request to the card issuer server corresponding to the target account information, the method further includes:

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

receiving the data processing request forwarded by the acquirer server.

[0012] In an optional embodiment, before receiving the target biometric information and the verification password information of the target object, the method further includes:

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.

[0013] In an optional embodiment, the storing the encrypted routing index information, the registered biometric information and the registered account information of the target object

associatively includes:

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

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

[0014] The determining the target account information of the target object includes:

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

10 **[0015]** After determining the target account information of the target object, the method further includes:

sending the Tokent information to the terminal.

[0016] In an optional embodiment, the biometric information includes one or a plurality of the following listed items:

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

[0017] In a second aspect, the present disclosure provides a data processing apparatus, including:

20 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 recognize matched registered biometric information, matched with the target biometric information, from registered biometric information of a plurality of objects, wherein registered biometric information of any of the objects and registered account information of the any object are stored associatively; and

25 a determining component, configured to determine target account information of the target object according to the matched recognized registered biometric information.

[0018] 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 includes the target account information and the verification password information, so that
30 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.

[0019] In an optional embodiment, the recognition component is configured to:

35 determine partition biometric information from the registered biometric information of the plurality of objects, wherein the partition biometric information is registered biometric

information stored in association with the verification password information;

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

recognize the 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.

[0020] In an optional embodiment, 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.

[0021] In an optional embodiment, 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, wherein the auxiliary recognition information is sent by the terminal to the acquirer server in response to operation of a user.

[0022] 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 with the target biometric information, from the registered biometric information corresponding to the auxiliary recognition information.

[0023] In an optional embodiment, the transceiving component is further configured to:

send the target account information to the terminal through the acquirer server, so that the terminal sends the data processing request to the acquirer server, wherein the data processing request includes the target account information and the verification password information; and

receive the data processing request forwarded by the acquirer server.

[0024] In an optional embodiment, the apparatus further includes a registration component, which is 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;
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.

[0025] In an optional embodiment, 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.

[0026] 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.

[0027] The transceiving component is further configured to send the Token information to the terminal.

[0028] In an optional embodiment, the biometric information includes one or a plurality of the following listed items:

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

[0029] In a third aspect, the present disclosure further provides an electronic device, including:
at least one processor; and
a memory in communication connection with the at least one processor.

[0030] 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, so that the above method may be executed by the at least one processor.

[0031] In a fourth aspect, the present disclosure further provides a non-transitory computer readable storage medium, storing computer instructions, wherein the computer instructions are configured to make a computer execute the above method.

[0032] In a fifth aspect, the present disclosure further provides a data processing system, including an acquirer server, a biometric recognition server and a card issuer server.

[0033] 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

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

5 **[0083]** During implementations, after the partition biometric information corresponding to the verification password information is determined from all the registered biometric information, the quantity of the partition biometric information needs to be determined, and the quantity of the partition biometric information is compared with the quantity threshold value. For example, if there are P partition biometric information and the quantity threshold value is 500, P is compared
10 with 500, if P is smaller than 500, the P partition biometric information is directly compared with the target biometric information respectively, and the registered biometric information matched with the target biometric information is searched out from the P partition biometric information; and if P is larger than or equal to 500, it indicates that the quantity of the partition biometric information is still large, the recognition range needs to be further narrowed down. For example,
15 a least recently used (LRU) algorithm may be used, and part of the partition biometric information is selected as the sub-partition biometric information. For example, Q partition biometric information is selected from the P partition biometric information to serve as the sub-partition biometric information, $Q \leq P$. Then, the Q sub-partition biometric information is compared with the target biometric information respectively, and the registered biometric information matched
20 with the target biometric information is recognized from the Q sub-partition biometric information.

[0084] In embodiments of the present disclosure, the registered biometric information matched with the target biometric information is determined through a corresponding relation between the verification password information and the registered biometric information, the biometric
25 recognition range may be narrowed down, the recognition computation amount is greatly reduced, and the recognition success rate is increased.

[0085] However, if the quantity of the sub-partition biometric information is still large, the probability of failure in the process of recognizing the registered biometric information matched with the target biometric information still exist. In embodiments of the present disclosure, if
30 executing the step of recognizing the registered biometric information matched with the target biometric information fails (namely, there is no registered biometric information matched with the target biometric information), a recognition failure response may be sent to the terminal through the acquirer server, so that the terminal displays a prompt of inputting auxiliary recognition information. A specific implementation process is as follows.

35 **[0086]** The auxiliary recognition information forwarded by the acquirer server is received. The

auxiliary recognition information is sent by the terminal to the acquirer server in response to operation of the user.

[0087] Registered biometric information corresponding to the auxiliary recognition information is determined from the sub-partition biometric information through the auxiliary recognition information.

[0088] Registered biometric information matched with the target biometric information is recognized from registered biometric information corresponding to the auxiliary recognition information.

[0089] The auxiliary recognition information may be last four digits of a mobile phone number of the user, first six digits of an ID number of the user, and the like. There is also a corresponding relation between the auxiliary recognition information and the registered biometric information, namely, one piece of auxiliary recognition information corresponds to a plurality of registered biometric information. If the quantity of the sub-partition biometric information selected out from the partition biometric information through the algorithm is still large, the registered biometric information matched with the target biometric information still cannot be recognized. In this case, the registered biometric information corresponding to the auxiliary recognition information may be found from the sub-partition biometric information corresponding to the verification password information through the auxiliary recognition information, thus on the basis of narrowing down the recognition range through the verification password information and the algorithm, the recognition range may be further narrowed down through the auxiliary recognition information, and the recognition success rate is improved.

[0090] For example, if recognition fails, the biometric recognition server sends a recognition failure feedback to the acceptance terminal through the acquirer server, the acceptance terminal prompts the user to input the last four digits of the mobile phone number as the auxiliary recognition information, and thus the recognition range is further narrowed down.

[0091] Fig. 4 illustrates a process of determining target account information by a biometric recognition server. As shown in Fig. 4, hypothetically, a face image received by the biometric recognition server is a living body picture of the user A, and the payment password is 217384. That is, the target biometric information is the living body picture. The payment password is computed through an irreversible algorithm and then transformed into a security code 2ac59075b9. N face images are stored in a face route library, and M face images corresponding to the security code 2ac59075b9 are determined from the N face images. M is compared with a preset quantity 500, if $M \leq 500$, face identification is directly performed between the received living body picture and each of the M stored face images, a face image of the user A is recognized from the M face images, and then a bank card Token of the user A is obtained. If $M > 500$, Q face

images are selected out from the M face images through the LRU algorithm, so that a subset library is formed. The Q face images are respectively compared with the received living body picture, if recognition is successful, the face image of the user A is obtained, and then the bank card Token of the user A is obtained. If recognition fails, the last four digits of the mobile phone of the user are obtained so as to further narrow down the recognition range, the face image of the user A is obtained, and then the bank card Token of the user A is obtained.

[0092] In order to utilize existing system resources to the maximum degree, in embodiments of the present disclosure, whole transaction is divided into a recognition process and a data processing process. Before the biometric recognition server sends the data processing request to the card issuer server corresponding to the target account information, the method further includes the following operations.

[0093] The target account information is sent to the terminal through the acquirer server, so that the terminal sends the data processing request to the acquirer server. The data processing request includes the target account information and the verification password information.

[0094] The data processing request forwarded by the acquirer server is received.

[0095] During implementations, as for one transaction, the acceptance terminal may send two requests, namely one recognition request and one payment request. For example, the acceptance terminal generates the recognition request in response to the operation of the user and sends the recognition request to the biometric recognition server through the acquirer server. The recognition request includes the target biometric information and the verification information of the user. Then, the acceptance terminal generates the payment request after receiving the target account information sent by the biometric recognition server and sends the payment request to the card issuer server through the acquirer server and the biometric recognition server. The payment request includes the target account information and the verification password information.

The biometric recognition server may be a server in a clearing mechanism. As in an existing transaction system, the clearing mechanism server is connected with the card issuer server and data in the card issuer server are synchronous with the clearing mechanism server, thus, this system structure and the processing manner of one transaction and two requests make small change to the existing system, the existing system resources may be utilized to the maximum degree, and any overlaying onto an existing data processing type is allowed, for example, fund transfer, cash withdrawal, pre-authorization and other types of transactions, and no modification is needed.

[0096] Fig. 5 illustrates a schematic diagram of a data flow direction provided by an embodiment of the present disclosure. As shown in Fig. 5, the acceptance terminal receives the face image and the payment password of the user through step 1, and then the acceptance terminal sends the face image and the payment password to a face route gateway in the clearing mechanism

information after receiving the verification password information, and the registered account information, the registered biometric information and the routing index information are synchronous with the biometric recognition server. The biometric recognition server performs salt encryption processing on the routing index information of each user so as to ensure the information security. Salt encryption is a data encryption mode, for example, each of data is associated with an n-digit random number called 'salt' for together encryption. The random changes as long as the data change whenever possible. The random number is stored in a file in an unencrypted mode, an encrypted result is also stored in the file. The irreversible algorithm may be SM3, SHA-256 and the like.

[00104] Fig. 6 illustrates a registration flow provided by an embodiment of the present disclosure. As shown in Fig. 6, the user sets the payment password in a card issuing bank APP. The card issuing banking business system operates the payment password to a face payment security code through irreversible operation, and then the face payment security code is synchronous with a face route platform. The face route platform adds different salt into each face payment security code and performs encrypted storage.

[00105] In order to further ensure the data storage and transmission security, 'the encrypted routing index information, the registered biometric information and the registered account information are stored associatively' in the above content may include the following operations.

[00106] Tokenization processing is performed on the registered account information so as to obtain card Tokend information.

[00107] The encrypted routing index information, the registered biometric information and the Tokend information are stored associatively.

[00108] Correspondingly, determining the target account information of the target object, includes the following operations.

[00109] Tokend information corresponding to the target biometric information is determined.

[00110] The Tokend information is converted into Token information.

[00111] Furthermore, after the target account information of the target object is determined, the method further includes: sending the Token information to the terminal.

[00112] During implementations, in order to prevent leakage of the account information of the user, tokenization processing may be performed on the account information so as to generate Token information. In an optional embodiment, the card Token information may be generated by means of a payment tokenization service (Token service provider (TSP)), the payment tokenization service TSP is a digital payment basic security service and may provide security guarantee for payments of a bank, a payment institution and an industry body. The payment tokenization service TSP uses a specific payment Token to replace a traditional bank card number,

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

[00134] In an optional embodiment, the transceiving component 901 is further configured to:

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

[00135] In an optional embodiment, the apparatus further includes a registration component 904, 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; perform salt encryption processing on the routing index information; and store encrypted routing index information, the registered biometric information and the registered account information associatively.

[00136] In an optional embodiment, the registration component 904 is configured to perform tokenization processing on the registered account information so as to obtain Tokend information; and store the encrypted routing index information, the registered biometric information and the Tokend information associatively.

[00137] The determining component 903 is further configured to determine Tokend information corresponding to the target biometric information; and convert the Tokend information into the Token information.

[00138] The transceiving component 901 is further configured to send the Token information to the terminal.

[00139] In an optional embodiment, the biometric information includes one or a plurality of the following listed items:

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

[00140] Based on the same principle, the present disclosure further provides an electronic device, as illustrated in Fig. 10, including: a processor 701, a memory 702, a transceiver 703 and a bus interface (704). The processor 701, the memory 702 and the transceiver 703 are connected through the bus interface 704.

[00141] The processor 701 is configured to read program(s) in the memory 702 and execute the following method.

[00142] Target biometric information and verification password information of a target object

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;

recognizing matched registered biometric information, matched with the target biometric
information, from registered biometric information of a plurality of objects, wherein registered
biometric information of any of the objects and registered account information of the any object
are associatively stored;

10 determining target account information of the target object according to the matched
registered biometric information; and

sending 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
15 the verification password information and performs data processing according to the target
account information after the verification is passed.

2. The method according to claim 1, wherein the recognizing matched registered biometric
information, matched with the target biometric information, from registered biometric
20 information of a plurality of objects comprises:

determining partition biometric information from the registered biometric information of the
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
25 corresponding to the verification password information;

recognizing the 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

verifying a recognition result of the main recognition algorithm through the auxiliary
30 recognition algorithm.

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

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

 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;

10 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.

4. The method according to claim 3, comprising:

15 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 of inputting auxiliary recognition information;

20 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 information from the sub-partition biometric information; and

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

5. 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:

30 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

request comprises the target account information and the verification password information; and
receiving the data processing request forwarded by the acquirer server.

6. 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:

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.

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

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

converting the Tokend information corresponding to the target biometric information
into Token information; and

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

sending the Token information to a terminal.

8. The method according to any of claims 1 to 7, 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.

9. A data processing apparatus, comprising:

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

a recognition component, configured to recognize matched registered biometric information,
matched with the target biometric information, from registered biometric information of a
plurality of objects, wherein registered biometric information of any of the objects and registered
account information of the any object are associatively stored; and

10 a determining component, configured to determine target account information of the target
object according to the matched recognized registered biometric information; 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
15 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.

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

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

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

25 recognize the 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.

30

11. The apparatus according to claim 10, wherein the recognition component is configured to:

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

5 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

10 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.

12. The apparatus according to claim 11, wherein

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

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

25 13. The apparatus according to claim 9, wherein the transceiving component is further configured to:

30 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.

14. The apparatus according to claim 9, 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;

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.

15. The apparatus according to claim 14, wherein

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.

16. The apparatus according to any of claims 9 to 15, 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.

17. 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 8.

18. 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
5 claims 1 to 8.

19. 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
10 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; recognize matched registered biometric information, matched with the target biometric information, from registered biometric
15 information of a plurality of objects, wherein registered biometric information of any of the object and registered account information of the any object are stored associatively; 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 server corresponding to the target account information, wherein the data processing request comprises the target account
20 information and the verification password information; and

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.