

BIOMETRIC MATCHING METHOD, TERMINAL DEVICE, SERVER, SYSTEM, AND MEDIUM

CROSS REFERENCE TO RELATED APPLICATION

[0001] The present application claims priority to Chinese Patent Application No. 202310095121.8 filed on January 20, 2023, and titled “BIOMETRIC MATCHING METHOD, TERMINAL DEVICE, SERVER, SYSTEM, AND MEDIUM”, which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The present application belongs to the field of data processing, and particularly relates to a biometric matching method, terminal device, server, system, and medium.

BACKGROUND

[0003] With the development of information technology, biometric identification technology such as face recognition is widely used in identity authentication, forensic verification, and other scenarios. A matching using the biometric identification technology requires collecting user's biometric data in advance and uploading the biometric data to a server as a matching sample, and when performing biometric matching for the user, the currently collected biometric data are compared with the biometric data as the matching sample to achieve the biometric matching.

[0004] However, the user's biometrics are privacy data for the user, and thus any leakage of the matching sample stored in the server or the biometric data in the uploading process will bring a great risk to the user's data security.

SUMMARY

[0005] Embodiments of the present application provide a biometric matching method, terminal device, server, system, and medium, which can reduce the security risk of the user's privacy data.

[0006] In a first aspect, the embodiments of the present application provide a biometric

matching method applied to a terminal device, the method including: performing, based on a first private key, an acquired biometric vector to be matched, a preset generating element, a second private key, and first encrypted data, a number of interactions and processes with a server to obtain second encrypted data, the first private key being a private key for the terminal device, the second private key being a private key for the server, the first encrypted data being pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server, a computational operator including the second private key and a target Euclidean distance being formed in the second encrypted data, the target Euclidean distance including a Euclidean distance between the biometric vector to be matched and the sample biometric vector; and sending the second encrypted data to the server to cause the server to obtain, using the second encrypted data, the generating element, the second private key, and a preset Euclidean distance matching threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

[0007] In a second aspect, the embodiments of the present application provide a biometric matching method applied to a server, the method including: performing, based on a second private key, first encrypted data, a first private key, a preset generating element, and a biometric vector to be matched acquired by a terminal device, a number of interactions and processes with the terminal device to cause the terminal device to obtain second encrypted data, the first private key being a private key for the terminal device, the second private key being a private key for the server, the first encrypted data being pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server, a computational operator including the second private key and a target Euclidean distance being formed in the second encrypted data, the target Euclidean distance including a Euclidean distance between the biometric vector to be matched and the sample biometric vector; receiving the second encrypted data sent by the terminal device; and obtaining, using the second encrypted data, the second private key, the generating element, and a preset Euclidean distance matching threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

[0008] In a third aspect, the embodiments of the present application provide a terminal device including a first communication module and a first encryption module; the first communication

module and the first encryption module being configured to perform, based on a first private key, an acquired biometric vector to be matched, a preset generating element, a second private key, and first encrypted data, a number of interactions and processes with a server to obtain second encrypted data, the first private key being a private key for the terminal device, the second private key being a private key for the server, the first encrypted data being pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server, a computational operator including the second private key and a target Euclidean distance being formed in the second encrypted data, the target Euclidean distance including a Euclidean distance between the biometric vector to be matched and the sample biometric vector; and the first communication module being further configured to send the second encrypted data to the server to cause the server to obtain, using the second encrypted data, the generating element, the second private key, and a preset Euclidean distance matching threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

[0009] In a fourth aspect, the embodiments of the present application provide a server including a second communication module, a second encryption module, and a matching module; the second communication module and the second encryption module being configured to perform, based on a second private key, first encrypted data, a first private key, a preset generating element, and a biometric vector to be matched acquired by a terminal device, a number of interactions and processes with the terminal device to cause the terminal device to obtain second encrypted data, the first private key being a private key for the terminal device, the second private key being a private key for the server, the first encrypted data being pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server, a computational operator including the second private key and a target Euclidean distance being formed in the second encrypted data, the target Euclidean distance including a Euclidean distance between the biometric vector to be matched and the sample biometric vector; the second communication module being further configured to receive the second encrypted data sent by the terminal device; and the matching module being configured to obtain, using the second encrypted data, the second private key, the generating element, and a preset Euclidean distance matching

threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

[0010] In a fifth aspect, the embodiments of the present application provide a terminal device including: a processor and a memory storing computer program instructions; and the processor implementing, when executing the computer program instructions, the biometric matching method of the first aspect.

[0011] In a sixth aspect, the embodiments of the present application provide a server including: a processor and a memory storing computer program instructions; and the processor implementing, when executing the computer program instructions, the biometric matching method of the second aspect.

[0012] In a seventh aspect, the embodiments of the present application provide a biometric matching system including the terminal device of the fifth aspect and the server of sixth aspect.

[0013] In an eighth aspect, the embodiments of the present application provide a computer-readable storage medium storing computer program instructions thereon, the computer program instructions, when executed by a processor, implementing the biometric matching method of the first aspect or the biometric matching method of the second aspect.

[0014] The embodiments of the present application provide a biometric matching method, terminal device, server, system, and medium, in which a number of interactions and processes may be performed between the terminal device and the server based on the first private key, the biometric vector to be matched, the generating element, the second private key, and the first encrypted data, the terminal device has the first private key, the biometrics to be matched, and the generating element, and the server has the second private key and the first encrypted data. With the encryption process by the terminal device using the first private key, the encryption process by the server using the second private key, and the data interaction between the terminal device and the server, the terminal device can obtain the second encrypted data having the computational operator including the second private key and the target Euclidean distance which can characterize the Euclidean distance between the biometric vector to be matched and the sample biometric vector, the second encrypted data contains the second private key, while the terminal device cannot learn the second private key and thus cannot crack and obtain the plaintext of the biometric vector to be matched and the sample biometric vector, and similarly,

the server cannot learn the first private key and thus cannot crack the first encryption private key. Moreover, the server determines the matching result for the biometric vector to be matched and the sample biometric vector according to the second encrypted data, the generating element, the second private key, and the preset Euclidean distance matching threshold, and the matching can be achieved without involving the plaintext of the biometric vector to be matched and the plaintext of the sample biometric vector, thereby reducing the security risk of the user's privacy data and improving the security of the biometric matching.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] In order to illustrate the technical solutions of the embodiments of the present application more clearly, the drawings necessary for the embodiments of the present application will be introduced briefly below. For those of ordinary skills in the art, other drawings can be obtained from these drawings without any inventive effort.

[0016] Fig. 1 shows a schematic architectural diagram of a biometric matching system according to the embodiments of the present application;

[0017] Fig. 2 shows a flowchart of a biometric matching method according to an embodiment of the first aspect of the present application;

[0018] Fig. 3 shows a flowchart of a biometric matching method according to another embodiment of the first aspect of the present application;

[0019] Fig. 4 shows a flowchart of a biometric matching method according to an embodiment of the second aspect of the present application;

[0020] Fig. 5 shows a flowchart of a biometric matching method according to another embodiment of the second aspect of the present application;

[0021] Fig. 6 shows a schematic structural diagram of a terminal device according to an embodiment of the third aspect of the present application;

[0022] Fig. 7 shows a schematic structural diagram of a server according to an embodiment of the fourth aspect of the present application;

[0023] Fig. 8 shows a schematic structural diagram of a terminal device according to an embodiment of the fifth aspect of the present application;

[0024] Fig. 9 shows a schematic structural diagram of a server according to an embodiment

of the sixth aspect of the present application.

DETAILED DESCRIPTION

[0025] Features and exemplary embodiments of various aspects of the present application will be described in detail below. In order to make the objects, technical solutions and advantages of the present application clearer, the present application is further described in detail below with reference to the accompany drawings and specific embodiments. It should be understood that the specific embodiments described herein are only for illustrating the present application, rather than limiting the present application. For those skilled in the art, the present application can be implemented without some of those specific details. The below description of the embodiments is only for providing a better understanding of the present application by illustrating examples of the present application.

[0026] With the development of information technology, biometric identification technology such as face recognition is widely used in identity authentication, forensic verification, and other scenarios. A matching using the biometric identification technology requires collecting user's biometric data in advance and uploading the biometric data to a server as a matching sample, and when performing biometric matching for the user, the currently collected biometric data are compared with the biometric data as the matching sample to achieve the biometric matching. However, the user's biometrics are privacy data for the user, and thus any leakage of the matching sample stored in the server or the biometric data in the uploading process will bring a great risk to the user's data security.

[0027] The present application provides a biometric matching method, terminal device, server, system, and medium, in which the terminal device can encrypt the biometric vector using its own private key and interact with the server, and the server can encrypt the received data using its own private key. With the encryption process by the terminal device using its own private key and the encryption process by the server using its own private key, the encrypted data having the computational operator including the Euclidean distance which can characterize the similarity between the biometric vector to be matched and the sample biometric vector is constructed, and the matching result is obtained using this encrypted data, so that the matching of biometrics is achieved in the case that both the terminal device and the server do not store

the plaintext data of the biometrics, and thus the security risk of the user's privacy data is reduced and the security of the biometric matching is improved.

[0028] It should be noted that the acquisition, storage, use, and process of information and data in the present application are authorized by the user or the relevant organization, and are in compliance with the relevant provisions of national laws and regulations.

[0029] The biometric matching method, terminal device, server, system, and medium according to the embodiments of the present application may be applied to payment, clock in, traffic, and other scenarios requiring identity recognition, which is not limited herein. The biometric matching method, terminal device, server, system, and medium according to the present application are described below.

[0030] For ease of understanding, the system architecture to which the biometric matching method according to the embodiments of the present application is applied is first briefly described herein. Fig. 1 shows a schematic architectural diagram of a biometric matching system according to the embodiments of the present application, which may include a terminal device 11 and a server 12, as shown in Fig. 1.

[0031] The terminal device 11 may be a device used by the user and may be installed with applications requiring biometric identification function, or the operating system of the terminal device 11 itself requires the biometric identification function, which is not limited herein. The terminal device 11 may collect and process the biometric data of the user. For example, the terminal device 11 may include a cell phone, a tablet computer, a smart wearable device, a clock in device, a vending machine, and the like, and the type and number of the terminal device 11 are not limited herein. The terminal device 11 may communicate and interact with the server 12. In the embodiments of the present application, the terminal device 11 has its own private key, i.e., a first private key, which may be used to encrypt data.

[0032] The server 12 may communicate and interact with the terminal device 11 to receive data transmitted from the terminal device 11. The server 12 stores sample biometric data in the form of cipher text, and the sample biometric data includes biometric data as a matching sample or an identification sample. In the embodiments of the present application, the server 12 has its own private key, i.e., a second private key, which may be used to encrypt data. The server 12 may obtain a matching result and back feed the matching result to the terminal device 11. The

type and number of the server 12 are not limited herein.

[0033] The first aspect of the present application provides a biometric matching method which may be applied to a terminal device, that is, the biometric matching method may be executed by the terminal device. Fig. 2 shows a flowchart of a biometric matching method according to an embodiment of the first aspect of the present application, and as shown in Fig. 2, the biometric matching method may include step S201 and step S202.

[0034] Step S201: performing, based on a first private key, an acquired biometric vector to be matched, a preset generating element, a second private key, and first encrypted data, a number of interactions and processes with a server to obtain second encrypted data.

[0035] The terminal device has the first private key, the biometric vector to be matched, and the generating element. The first private key is a private key for the terminal device and cannot be learned by the server. The biometric vector to be matched is a vector transformed from the biological data to be matched. The terminal device may collect the biological data to be matched, which is the original biological data to be matched, and the terminal device may transform the biological data to be matched to the biometric vector to be matched using a vector transformation model. The biological data to be matched may include one or more of face data, fingerprint data, palm vein data, iris data, etc., and is not limited herein. A transformation model matching the type of the original biological data may be selected as the vector transformation model, and the type of the vector transformation model is not limited herein. For example, the biological data to be matched includes face data which may specifically be face image data, and a model such as OpenFace, Eigenface may be selected to perform feature extraction on the face data and form a face feature vector.

[0036] The server has the second private key and the first encrypted data. The second private key is a private key for the server and cannot be learned by the terminal device. The first encrypted data may be pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server. The terminal device may transform the acquired sample biological data to the sample biometric vector. The sample biological data may include one or more of face data, fingerprint data, palm vein data, iris data, etc., and is not limited herein. The vector transformation model for transforming the sample biological data to the sample biometric vector may be the consistent

with the vector transformation model for transforming the biological data to be matched to the biometric vector to be matched. The generating element may be pre-agreed upon by both the terminal device and the server and used as one of the base data involved in the respective encryption processes of the terminal device and the server.

[0037] The terminal device may encrypt the biometric vector to be matched using the generating element and the first private key, or may encrypt the data transmitted from the server. The data encrypted by the terminal device may be sent to the server to cause the server to encrypt the data transmitted from the terminal device, and the server may perform the encryption process using the second private key. With the encryption processes and the data interaction between the terminal device and the server, second encrypted data may be constructed at the terminal device. The second encrypted data is obtained substantially based on the encryption process of the data by the terminal device, the encryption process of the data by the server, and the interaction between the terminal device and the server. A computational operator including the second private key and a target Euclidean distance is formed in the second encrypted data. The target Euclidean distance includes a Euclidean distance between the biometric vector to be matched and the sample biometric vector and may characterize the similarity between the biometric vector to be matched and the sample biometric vector, and the smaller the target Euclidean distance, the higher the similarity between the biometric vector to be matched and the sample biometric vector, and the higher the possibility that the user corresponding to the biometric vector to be matched and the user corresponding to the sample biometric vector are the same user.

[0038] The computational operator may be regarded as a constituent of the data obtained by a computational process, and the computational process herein is a general computational process and may include a variety of computational process manners, such as encryption process, transformation process, mapping process, determine process, etc., all of which may be regarded as a computational process. As an example, parameter A, parameter B, and parameter C are involved in a computational process and data $AC \times (A+B)$ is obtained, then both AC and $(A+B)$ may be computational operators formed in the data, in which the computational operator AC may be a computational operator including A or a computational operator including C. As another example, parameter A, parameter B, and parameter C are involved in a computational

process and data A^{BC} is obtained, then BC may be a computational operator formed in the data, in which the computational operator BC may be a computational operator including B or a computational operator including C. In some examples, the computational operator may include a modular exponentiation operator or a dot product operator. The modular exponentiation operator is a computational operator in the form of exponentiation, e.g., in the data A^{BC} , a modular exponentiation operator BC including B is formed or a modular exponentiation operator BC including C is formed. The dot product operator is an operator in the form of a product, e.g., in the data $AC \times (A+B)$, AC and $(A+B)$ may be dot product operators, and the computational operator AC may be regarded as a dot product operator including A or a dot product operator including C. The computational operator including the second private key and the target Euclidean distance is formed in the second encrypted data, assuming that the second private key is b, the biometric vector to be matched is an n-dimensional vector $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$, the sample biometric vector is an n-dimensional vector $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$, and correspondingly, the Euclidean distance between the biometric vector to be matched and the sample biometric vector is $\sqrt{\sum_1^n (x_i - y_i)^2}$, then a computational operator including $b\sqrt{\sum_1^n (x_i - y_i)^2}$ may be formed in the second encrypted data. To facilitate the subsequent matching comparison, in some examples, the second encrypted data may include a computational operator $b\sum_1^n (x_i - y_i)^2$, which includes $b\sqrt{\sum_1^n (x_i - y_i)^2}$.

[0039] In some examples, the first private key may be a random number generated by the terminal device, and the second private key may be a random number generated by the server. To further improve data security, the first private key may be a large integer occupying at least 128 bits, e.g., the first private key may be a large integer occupying 256 bits; similarly, the second private key may be a large integer occupying at least 128 bits, e.g., the second private key may be a large integer occupying 256 bits. By setting the first private key and the second private key with a bit number greater than or equal to 128, the requirement for cryptographic security strength can be satisfied, the security of the user's personal privacy data can be further improved, and the security of biometric matching can also be further improved.

[0040] Step 202: sending the second encrypted data to the server to cause the server to obtain,

using the second encrypted data, the second private key, the generating element, and a preset Euclidean distance matching threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

[0041] The server may construct, using the second private key, the generating element, and the preset Euclidean distance matching threshold, data consistent with the second encrypted data format, and obtain, by comparing the second encrypted data with the data constructed using the second private key, the generating element, and the preset Euclidean distance matching threshold, the matching result for the biometric vector to be matched and the sample biometric vector. The preset Euclidean distance matching threshold is a determining threshold of the Euclidean distance for determining whether two vectors are the same vector, which may be set according to the scenario, demand, experience, etc., and is not limited herein. If the target Euclidean distance is less than or equal to the preset Euclidean distance matching threshold, it is indicated that the biometric vector to be matched and the sample biometric vector are successfully matched, i.e., the matching result is a successful match; if the target Euclidean distance is greater than the preset Euclidean distance matching threshold, it is indicated that the biometric vector to be matched and the sample biometric vector are failed to be matched, i.e., the matching result is a failed match. The second encrypted data contains the computational operator including the second private key and the target Euclidean distance, and the data constructed by the server using the second private key, the generating element, and the preset Euclidean distance matching threshold contains the computational operator including the second private key and the preset Euclidean distance matching threshold, and thus the comparison result between the second encrypted data and the data constructed by the server using the second private key, the generating element, and the preset Euclidean distance matching threshold and the comparison result between the target Euclidean distance and the preset Euclidean distance matching threshold are corresponding to each other, the comparison result between the target Euclidean distance and the preset Euclidean distance matching threshold are corresponding to each other may be determined by the comparison result between the second encrypted data and the data constructed by the server using the second private key, the generating element, and the preset Euclidean distance matching threshold, and this comparison result may characterize the matching result.

[0042] In the embodiments of the present application, a number of interactions and processes may be performed between the terminal device and the server based on the first private key, the biometric vector to be matched, the generating element, the second private key, and the first encrypted data, the terminal device has the first private key, the biometrics to be matched, and the generating element, and the server has the second private key and the first encrypted data. With the encryption process by the terminal device using the first private key, the encryption process by the server using the second private key, and the data interaction between the terminal device and the server, the terminal device can obtain the second encrypted data having the computational operator including the second private key and the target Euclidean distance which can characterize the Euclidean distance between the biometric vector to be matched and the sample biometric vector, the second encrypted data contains the second private key, while the terminal device cannot learn the second private key and thus cannot crack and obtain the plaintext of the biometric vector to be matched and the sample biometric vector, and similarly, the server cannot learn the first private key and thus cannot crack the first encryption private key. Moreover, the server determines the matching result for the biometric vector to be matched and the sample biometric vector according to the second encrypted data, the generating element, the second private key, and the preset Euclidean distance matching threshold, and the matching can be achieved without involving the plaintext of the biometric vector to be matched and the plaintext of the sample biometric vector, thereby reducing the security risk of the user's privacy data and improving the security of the biometric matching. Since the terminal device and the server do not store the plaintext of the biometric vector to be matched and the plaintext of the sample biometric vector, the user's control over the personal privacy data can be ensured, thereby restricting the scenario in which the personal privacy data is used, satisfying the minimized usage principle of the personal privacy data, and preventing the personal privacy data from being abused.

[0043] Moreover, in the embodiments of the present application, the biometric vector to be matched and the sample biometric vector are encrypted, the matching result is determined by the comparison of the encrypted data, the biological data to be matched and the sample biological data are of different types, and the vector transformation models that can be adopted may also be different, while in the embodiments of the present application, the similarity of the

biological data is described by the similarity of the feature vectors. During the matching of biometrics in the embodiments of the present application, the process of protecting personal privacy data and the transformation processes from the biological data to be matched to the biometric vector to be matched and from the sample biological data to the sample biometric vector may be independent of each other, thereby achieving a composable and pluggable technical solution for the vector transformation model and the biometric matching model, i.e., achieving decoupling between the vector transformation model and the biometric matching model.

[0044] In some embodiments, during the interactions and processes between the terminal device and the server, a plurality of intermediate encrypted data may be generated and the second encrypted data may be obtained by further processing the plurality of intermediate encrypted data. Fig. 3 shows a flowchart of a biometric matching method according to another embodiment of the first aspect of the present application, and Fig. 3 differs from Fig. 2 in that step S201 in Fig. 2 may be specifically refined into step S2011 to step S2013 in Fig. 3.

[0045] Step S2011: receiving first intermediate encrypted data sent by the server.

[0046] The first intermediate encrypted data is obtained by the server through encrypting the first encrypted data using the second private key. Computational operators including the first private key and elements in the sample biometric vector may be formed in the first encrypted data. Further, computational operators including products of the first private key and the elements in the sample biometric vector may be formed in the first encrypted data. For example, the first private key is a , the sample biometric vector is an n -dimensional vector $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$, the first encrypted data may include computational operators ay_i , and the first encrypted data may include computational operators ay_i^2 , $i=1, 2, \dots, n$; it should be noted that the computational operators ay_i^2 also includes the computational operators ay_i^2 .

[0047] The server may obtain the first intermediate encrypted data through encrypting the first encrypted data using the second private key. Computational operators including products of the first private key, the second private key, and the elements in the sample biometric vector may be formed in the first intermediate encrypted data. The first encrypted data has the computational operators including the products of the first private key and the elements in the

sample biometric vector, and the second private key may be used for encryption, so that the computational operators including the products of the first private key and the elements in the sample biometric vector are further multiplied by the second private key, so as to obtain the first intermediate encrypted data having the computational operators including the products of the first private key, the second private key, and the elements in the sample biometric vector. For example, the first private key is a , the second private key is b , the sample biometric vector is an n -dimensional vector $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$, and the first intermediate encrypted data may include computational operators aby_i .

[0048] Step S2012: obtaining second intermediate encrypted data according to the first intermediate encrypted data, the biometric vector to be matched, the generating element, and the first private key.

[0049] At least part of the data in the second intermediate encrypted data may be obtained based on the first intermediate encrypted data, and computational operators including products of the first private key and elements in the biometric vector to be matched are formed in the second intermediate encrypted data. For example, the first private key is a , the biometric vector to be matched is an n -dimensional vector $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$, and computational operators including ax_i may be formed in the second intermediate encrypted data. In order to be able to construct the second encrypted data in subsequent steps, the second intermediate encrypted data may be constructed further based on ax_i . The second intermediate encrypted data is used to participate in constructing the target Euclidean distance in subsequent steps.

[0050] In some examples, the second intermediate encrypted data includes first intermediate encrypted subdata and second intermediate encrypted subdata. Step S2012 may be specifically refined as: obtaining the first intermediate encrypted subdata according to the first intermediate encrypted data and the biometric vector to be matched; and obtaining the second intermediate encrypted subdata according to the first private key, the generating element, and the biometric vector to be matched.

[0051] Computational operators including products of the first private key, the second private key, elements in the sample biometric vector, and elements in the biometric vector to be matched are formed in the first intermediate encrypted subdata. For example, the first private

key is a , the second private key is b , the sample biometric vector is an n -dimensional vector $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$, the biometric vector to be matched is an n -dimensional vector $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$, the first intermediate encrypted subdata may form computational operators including abx_iy_i , and in order to be able to construct the target Euclidean distance in subsequent process, the first intermediate encrypted subdata may include computational operators $-2abx_iy_i$.

[0052] Computational operators including products of the first private key, the second private key, and elements in the biometric vector to be matched are formed in the second intermediate encrypted subdata. For example, the first private key is a , the biometric vector to be matched is an n -dimensional vector $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$, the second intermediate encrypted data may form computational operators including ax_i , and in order to be able to construct the target Euclidean distance in subsequent process, the second intermediate encrypted data may include computational operators ax_i^2 .

[0053] Step S2013: performing, based on the second intermediate encrypted data, the first encrypted data, the first private key, and the second private key, interactions and processes with the server, and removing the first private key from the processed data to obtain the second encrypted data.

[0054] After the second intermediate encrypted data is obtained, the second intermediate encrypted data may be sent to the server to cause the server to perform encryption process based on the second intermediate encrypted data, and then the encrypted data is back fed to the terminal device, and then the terminal device processes the received data to obtain the second encrypted data. In the embodiments of the present application, the second encrypted data may be obtained based on the second intermediate encrypted data through the process performed by the terminal device, the process performed by the server, and the data interaction between the terminal device and the server.

[0055] In some examples, the second intermediate encrypted data may be sent to the server to cause the server to obtain third intermediate encrypted data based on the second intermediate encrypted data, the first encrypted data, and the second private key; the third intermediate encrypted data sent by the server is received; and the first private key is removed, using the first private key, from the third intermediate encrypted data to obtain the second encrypted data.

[0056] The server may perform calculation on the second intermediate encrypted data and the first encrypted data to obtain the third intermediate encrypted data. The second intermediate encrypted data includes the first intermediate encrypted subdata and the second intermediate encrypted subdata, and the specific contents of which may refer to the relevant description in the above embodiments and will not be repeated herein. The server may perform calculation on the first intermediate encrypted subdata, the second intermediate encrypted subdata, and the first encrypted data to obtain the third intermediate encrypted data. A computational operator including a product of the first private key, the second private key, and the target Euclidean distance is formed in the third intermediate encrypted data. For example, the first private key is a , the second private key is b , the biometric vector to be matched is an n -dimensional vector $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$, the sample biometric vector is an n -dimensional vector $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$, and the third intermediate encrypted data may form a computational operator including $ab\sqrt{\sum_1^n (x_i - y_i)^2}$, e.g., the third intermediate encrypted data may include the computational operator $ab \sum_1^n (x_i - y_i)^2$, and the computational operator $ab \sum_1^n (x_i - y_i)^2$ includes $ab\sqrt{\sum_1^n (x_i - y_i)^2}$. The server cannot recognize the first private key, and thus the third intermediate encrypted data is transmitted to the terminal device, and the terminal device having the first private key removes the first private key from the third intermediate encrypted data involving the first private key to obtain the second encrypted data. The specific contents of the second encrypted data may refer to the relevant description in the above embodiments, and will not be repeated herein.

[0057] With the interaction between the terminal device and the server, the terminal device and the server may respectively perform further process based on their received data, the second encrypted data is constructed through the interaction and re-process of the intermediate encrypted data, and the entire process does not involve the plaintext of the biometric vector to be matched and the plaintext of the sample biometric vector, which is safe and reliable.

[0058] In some embodiments, the server may determine whether the biometric vector to be matched and the sample biometric vector are successfully matched by determining whether the second encrypted data belongs to a matched data set. The matched data set may be generated by the server, and a maximum value of elements in the matched data set is obtained based on

the second private key and the preset Euclidean distance matching threshold. In some examples, a computational operator including a product of the second private key and the preset Euclidean distance matching threshold is formed in the maximum value of the elements in the matched data set, and the preset Euclidean distance matching threshold herein may be the preset Euclidean distance matching threshold itself or the preset Euclidean distance matching threshold after being converted to an integer, which is not limited herein.

[0059] The matching result includes a successful match under a condition that the second encrypted data belongs to the matched data set; and the matching result includes a failed match under a condition that the second encrypted data does not belong to the matched data set. The second encrypted data belonging to the matched data set indicates that the target Euclidean distance is less than or equal to the preset Euclidean distance matching threshold. The second encrypted data not belonging to the matched data set indicates that the target Euclidean distance is greater than the preset Euclidean distance matching threshold.

[0060] In some embodiments, the elements in the biometric vector to be matched, the elements in the sample biometric vector, and the preset Euclidean distance matching threshold are converted to integers by equal multiples. That is, after being converted to integers by equal multiples, the elements in the biometric vector to be matched, the elements in the sample biometric vector, and the preset Euclidean distance matching threshold are all integers, and the multiples relative to the original elements in the biometric vector to be matched, the original elements in the sample biometric vector, and the original preset Euclidean distance matching threshold are the same. Correspondingly, since the preset Euclidean distance matching threshold, after being converted to an integer by equal multiples, is an integer and the number of the elements in the matched data set is limited, computational operators including products of the second private key and each of 0 to a square of the preset Euclidean distance matching threshold after being converted to an integer are formed in the matched data set. For example, the second private key is b and the preset Euclidean distance matching threshold is θ , the computational operators that may be involved in the matched data set may include $b \times 0$, $b \times 1$, $b \times 2$,, $b \times \theta^2$.

[0061] In some embodiments, in order to improve the efficiency of biometric matching, a Bloom filter may be used to determine whether the second encrypted data belongs to the

matched data set. It may be determined that the second encrypted data belongs to the matched data set under a condition that values of positions in a pre-established Bloom filter lookup table corresponding to K target hash values are all 1; and it may be determined that the second encrypted data does not belong to the matched data set under a condition that at least one of the values of the positions in the Bloom filter lookup table corresponding to the K target hash values is 0.

[0062] Herein, the K target hash values are calculated based on the second encrypted data according to K hash functions. Calculation may be performed on each of the second encrypted data according to one hash function to obtain one target hash value. Each of the second encrypted data corresponds to K target hash values. K is a positive integer and may be set according to the scenario, demand, experience, etc., and is not limited herein. Values in the Bloom filter lookup table are calculated based on elements in the matched data set according to the K hash functions. The Bloom filter lookup table may be generated by the server. Specifically, the server may perform, using the K hash functions, calculation on each of the elements in the matched data set to obtain K hash values corresponding to the element; and map the K hash values corresponding to the element to K positions in a binary array whose values are all 0 and update values of the K positions corresponding to the element to 1, and determine the updated binary array as the Bloom filter lookup table. The K hash functions for generating the Bloom filter lookup table are the same as the K hash functions for calculating the K target hash values. In some examples, the binary array, before being updated, is a binary array with value 0 at each position, each position in the binary array may be represented by the subscript of the element in the binary array, the hash value corresponding to the element is mapped to the position in the binary array, and specifically, the hash value corresponding to the element may be mapped to the subscript of the element in the binary array.

[0063] Using the Bloom filter to determine whether the second encrypted data belongs to the matched data set may speed up the determination of whether the second encrypted data belongs to the matched data set, especially when the numbers of the biometric vectors to be matched and the sample biometric vectors are very huge, and thus the efficiency of biometric matching can be significantly improved.

[0064] In some embodiments, before performing the matching for the biometric vector to be

matched and the sample biometric vector, the terminal device may generate the first encrypted data and transmit the first encrypted data to the server to cause the server to store the first encrypted data. Specifically, the terminal device may acquire the sample biometric vector; encrypt the sample biometric vector using the generating element and the first private key to obtain the first encrypted data; and sent the first encrypted data to the server. Computational operators including products of the first private key and the elements in the sample biometric vector may be formed in the first encrypted data, which may refer to the relevant description in the above embodiments and will not be repeated herein.

[0065] The first encrypted data contains the first private key which cannot be learned by the server, and thus it is difficult to crack the first encrypted data at the server, and the security of personal privacy data stored in the server can be ensured.

[0066] The second aspect of the present application provides a biometric matching method which may be applied to a server, that is, the biometric matching method may be executed by the server. Fig. 4 shows a flowchart of a biometric matching method according to an embodiment of the second aspect of the present application, and as shown in Fig. 4, the biometric matching method may include step S301 to step S303.

[0067] Step S301: performing, based on a second private key, first encrypted data, a first private key, a preset generating element, and a biometric vector to be matched acquired by a terminal device, a number of interactions and processes with the terminal device to cause the terminal device to obtain second encrypted data.

[0068] The first private key is a private key for the terminal device. The second private key is a private key for the server. The first encrypted data is pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server. A computational operator including the second private key and a target Euclidean distance is formed in the second encrypted data. The target Euclidean distance includes a Euclidean distance between the biometric vector to be matched and the sample biometric vector.

[0069] In some examples, the computational operator may include a modular exponentiation operator or a dot product operator.

[0070] Step S302: receiving the second encrypted data sent by the terminal device.

[0071] Step S303: obtaining, using the second encrypted data, the second private key, the generating element, and a preset Euclidean distance matching threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

[0072] The specific contents of the above steps S301 to S303 may refer to the relevant description in the above embodiments, and will not be repeated herein.

[0073] In the embodiments of the present application, a number of interactions and processes may be performed between the server and the terminal device based on the first private key, the biometric vector to be matched, the generating element, the second private key, and the first encrypted data, the terminal device has the first private key, the biometrics to be matched, and the generating element, and the server has the second private key and the first encrypted data. With the encryption process by the terminal device using the first private key, the encryption process by the server using the second private key, and the data interaction between the terminal device and the server, the terminal device can obtain the second encrypted data having the computational operator including the second private key and the target Euclidean distance which can characterize the Euclidean distance between the biometric vector to be matched and the sample biometric vector, the second encrypted data contains the second private key, while the terminal device cannot learn the second private key and thus cannot crack and obtain the plaintext of the biometric vector to be matched and the sample biometric vector, and similarly, the server cannot learn the first private key and thus cannot crack the first encryption private key. Moreover, the server determines the matching result for the biometric vector to be matched and the sample biometric vector according to the second encrypted data, the generating element, the second private key, and the preset Euclidean distance matching threshold, and the matching can be achieved without involving the plaintext of the biometric vector to be matched and the plaintext of the sample biometric vector, thereby reducing the security risk of the user's privacy data and improving the security of the biometric matching. Since the terminal device and the server do not store the plaintext of the biometric vector to be matched and the plaintext of the sample biometric vector, the user's control over the personal privacy data can be ensured, thereby restricting the scenario in which the personal privacy data is used, satisfying the minimized usage principle of the personal privacy data, and preventing the personal privacy data from being abused.

[0074] Moreover, in the embodiments of the present application, the biometric vector to be matched and the sample biometric vector are encrypted, the matching result is determined by the comparison of the encrypted data, the biological data to be matched and the sample biological data are of different types, and the vector transformation models that can be adopted may also be different, while in the embodiments of the present application, the similarity of the biological data is described by the similarity of the feature vectors. During the matching of biometrics in the embodiments of the present application, the process of protecting personal privacy data and the transformation processes from the biological data to be matched to the biometric vector to be matched and from the sample biological data to the sample biometric vector may be independent of each other, thereby achieving a composable and pluggable technical solution for the vector transformation model and the biometric matching model, i.e., achieving decoupling between the vector transformation model and the biometric matching model.

[0075] In some embodiments, during the interactions and processes between the server and the terminal device, a plurality of intermediate encrypted data may be generated and the second encrypted data may be obtained by further processing the plurality of intermediate encrypted data. Fig. 5 shows a flowchart of a biometric matching method according to another embodiment of the second aspect of the present application, Fig. 5 differs from Fig. 4 in that step S301 in Fig. 4 may be specifically refined into step S3011 to step S3013 in Fig. 5, and step S303 in Fig. 4 may be specifically refined into step S3031 to step S3033 in Fig. 5.

[0076] Step S3011: encrypting the first encrypted data using the second private key to obtain first intermediate encrypted data.

[0077] Computational operators including products of the first private key, the second private key, and elements in the sample biometric vector are formed in the first intermediate encrypted data.

[0078] Step S3012: sending the first intermediate encrypted data to the terminal device to cause the terminal device to obtain second intermediate encrypted data according to the first intermediate encrypted data, the biometric vector to be matched, the generating element, and the first private key.

[0079] Computational operators including products of the first private key and elements in

the biometric vector to be matched are formed in the second intermediate encrypted data.

[0080] In some examples, the second intermediate encrypted data includes first intermediate encrypted subdata and second intermediate encrypted subdata. The first intermediate encrypted subdata is obtained by the terminal device according to the first intermediate encrypted data and the biometric vector to be matched. Computational operators including products of the first private key, the second private key, elements in the sample biometric vector, and elements in the biometric vector to be matched are formed in the first intermediate encrypted subdata. The second intermediate encrypted subdata is obtained by the terminal device according to the first private key, the generating element, and the biometric vector to be matched. Computational operators including products of the first private key and elements in the biometric vector to be matched are formed in the second intermediate encrypted subdata.

[0081] Step S3013: performing, based on the second intermediate encrypted data, the first encrypted data, the first private key, and the second private key, interactions and processes with the terminal device to cause the terminal device to remove the first private key from the processed data to obtain the second encrypted data.

[0082] In some examples, step S3013 may be specifically refined into: receiving the second intermediate encrypted data sent by the terminal device; obtaining third intermediate encrypted data based on the second intermediate encrypted data, the first encrypted data, and the second private key, a computational operator including a product of the first private key, the second private key, and the target Euclidean distance being formed in the third intermediate encrypted data; and sending the third intermediate encrypted data to the terminal device to cause the terminal device to remove, using the first private key, the first private key from the third intermediate encrypted data to obtain the second encrypted data.

[0083] Step S3031: obtaining a matched data set based on the second private key, the generating element, and the preset Euclidean distance matching threshold.

[0084] A maximum value of elements in the matched data set is obtained based on the second private key and the preset Euclidean distance matching threshold.

[0085] In some examples, elements in the biometric vector to be matched, elements in the sample biometric vector, and the preset Euclidean distance matching threshold are converted to integers by equal multiples. Step S3031 may be specifically refined into: calculating

products of the second private key and each of 0 to a square of the preset Euclidean distance matching threshold after being converted to an integer; and obtaining the matched data set according to the products of the second private key and each of 0 to the square of the preset Euclidean distance matching threshold after being converted to an integer and the generating element.

[0086] Step S3032: determining that the matching result includes a successful match under a condition that the second encrypted data belongs to the matched data set.

[0087] Step S3033: determining that the matching result includes a failed match under a condition that the second encrypted data does not belong to the matched data set.

[0088] In some embodiments, the server may use a Bloom filter to determine whether the second encrypted data belongs to the matched data set. Specifically, the server may calculate K target hash values based on the second encrypted data according to K hash functions; determine that the second encrypted data belongs to the matched data set under a condition that values of positions in a pre-established Bloom filter lookup table corresponding to the K target hash values are all 1; and determine that the second encrypted data does not belong to the matched data set under a condition that at least one of the values of the positions in the Bloom filter lookup table corresponding to the K target hash values is 0. Herein, the K target hash values are calculated based on the second encrypted data according to the K hash functions, and values in the Bloom filter lookup table are calculated based on elements in the matched data set according to the K hash functions.

[0089] In some embodiments, the server may pre-generate the Bloom filter lookup table to facilitate determining whether the second encrypted data belongs to the matched data set using the Bloom filter. Specifically, the server may perform, using the K hash functions, calculation on each of the elements in the matched data set to obtain K hash values corresponding to the element; and map the K hash values corresponding to the element to K positions in a binary array whose values are all 0 and update values of the K positions corresponding to the element to 1, and determine the updated binary array as the Bloom filter lookup table.

[0090] The specific contents of the above steps S301 to S303 and steps S3031 to S3033 may refer to the relevant description in the above embodiments, and will not be repeated herein.

[0091] In the above embodiments, the computational operator may include a modular

exponentiation operator or a dot product operator. For ease of understanding, the registration and matching processes of biometrics are described below with examples in which the computational operator includes a modular exponentiation operator and a dot product operator, respectively. The registration process of biometrics refers to a process in which the terminal device processes data to obtain the first encrypted data and transmits the first encrypted data to the server which stores the first encrypted data, and the matching process of biometrics refers to a process in which the terminal device interacts with the server for a number of times to obtain a matching result for the biometric vector to be matched and the sample biometric vector.

[0092] In a first example, the computational operator includes a modular exponentiation operator, and the registration and matching processes of biometrics may include the following steps c1 to c12.

[0093] In step c1, the terminal device collects sample biological data and transforms the sample biological data to a sample biometric vector $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ with a vector transformation model.

[0094] In step c2, the terminal device generates a random number a as a first private key.

[0095] In step c3, the terminal device encrypts, using a generating element g and the first private key a , the sample biometric vector $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ to obtain first encrypted data.

[0096] The first encrypted data may include data g^{ay_i} and SY1 in the following equation (1), or may include data g^{ay_i} and $g^{ay_i^2}$ in the following equation (1), $i=1, 2, \dots, n$.

$$\text{[0097]} \quad \left\{ \begin{array}{l} y'_1 = g^{ay_1} \\ y'_2 = g^{ay_2} \\ \dots \dots \\ y'_n = g^{ay_n} \\ SY1 = g^{a(y_1^2 + y_2^2 + \dots + y_n^2)} \end{array} \right\} \quad (1)$$

[0098] In step c4, the first encrypted data is sent to and stored by the server.

[0099] The modular exponentiation operator is in the form of g^p , and the discrete logarithm problem in the field of cryptography may be used to ensure the security of the first encrypted data. That is, given an integer p in a finite field with a generating element g , it is easy to calculate $g^p = q$, but it is difficult to calculate p from g and q . The server cannot learn the first private key a , and due to the discrete logarithm problem, the server obtains g^{ay_i} , but

cannot crack and obtain y_i , and thus the first encrypted data is stored in the server in an encrypted state.

[00100] The above steps c1 to c4 belong to the registration process of biometrics.

[00101] In step c5, the terminal device collects biological data to be matched and transforms the biological data to be matched to a biometric vector to be matched $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$ with a vector transformation model.

[00102] In step c6, the server generates a random number b as a second private key.

[00103] In step c7, the server encrypts, using the second private key, the first encrypted data to obtain first intermediate encrypted data and sends the first intermediate encrypted data to the terminal device.

[00104] The first intermediate encrypted data may include g^{aby_i} in the following equation (2).

$$\textbf{[00105]} \quad \begin{cases} y''_1 = g^{aby_1} \\ y''_2 = g^{aby_2} \\ \dots \dots \\ y''_n = g^{aby_n} \end{cases} \quad (2)$$

[00106] In step c8, the terminal device obtains second intermediate encrypted data according to the biometric vector to be matched $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$, the first intermediate encrypted data, and the first private key, and sends the second intermediate encrypted data to the server.

[00107] The second intermediate encrypted data may include $g^{-2abx_iy_i}$ and $g^{ax_i^2}$ in the following equation (3).

$$\textbf{[00108]} \quad \begin{cases} (g^{aby_1})^{-2x_1} = g^{-2abx_1y_1} \\ (g^{aby_2})^{-2x_2} = g^{-2abx_2y_2} \\ \dots \dots \\ (g^{aby_n})^{-2x_n} = g^{-2abx_ny_n} \\ g^{a(x_1^2+x_2^2+\dots+x_n^2)} \end{cases} \quad (3)$$

[00109] In step c9, the server obtains third intermediate encrypted data using the second intermediate encrypted data, the first encrypted data, and the second private key b , and sends the third intermediate encrypted data to the terminal device.

[00110] The third intermediate encrypted data includes $g^{ab \sum_1^n (x_i - y_i)^2}$ in the following equation (4).

$$\begin{aligned}
[00111] \quad & g^{-2abx_1y_1} \times g^{-2abx_2y_2} \times \dots \times g^{-2abx_ny_n} \times g^{ab(x_1^2+x_2^2+\dots+x_n^2)} \times \\
& g^{ab(y_1^2+y_2^2+\dots+y_n^2)} = g^{ab \sum_1^n (x_i-y_i)^2}
\end{aligned} \tag{4}$$

[00112] It should be noted that, since the terminal device is considered as an untrusted party in the biometric matching scenario, the target Euclidean distance in an encrypted state must be constructed by the server.

[00113] In step c10, the terminal device removes, using the first private key, the first private key from the third intermediate encrypted data to obtain second encrypted data, and sends the second encrypted data to the server.

[00114] The second encrypted data includes $g^{b \sum_1^n (x_i-y_i)^2}$ in the following equation (5).

$$[00115] \quad (g^{ab \sum_1^n (x_i-y_i)^2})^{-a} = g^{b \sum_1^n (x_i-y_i)^2} \tag{5}$$

[00116] Since the terminal device cannot learn the second private key, the terminal device is unable to construct a computational operator including a Euclidean distance less than a preset Euclidean distance matching threshold, which further improves the security of data.

[00117] In step c11, the server obtains a matched data set $\{g^{b \times 0}, g^{b \times 1}, g^{b \times 2}, \dots, g^{b \times \theta^2}\}$ according to the second private key b and a preset Euclidean distance matching threshold θ .

[00118] Herein, the preset Euclidean distance matching threshold θ , as well as the previous sample biometric vector and biometric vector to be matched, may have been converted to integers by equal multiples, and thus the number of elements in this matched data set is limited.

[00119] In step c12, the server determines whether the second encrypted data $g^{b \sum_1^n (x_i-y_i)^2}$ is in the matched data set $\{g^{b \times 0}, g^{b \times 1}, g^{b \times 2}, \dots, g^{b \times \theta^2}\}$, if yes, it is determined that the biometric vector to be matched and the sample biometric vector are successfully matched; and if no, it is determined that the biometric vector to be matched and the sample biometric vector are failed to be matched.

[00120] The target Euclidean distance is $\sqrt{\sum_1^n (x_i - y_i)^2}$, and since the second encrypted data is in an encrypted state, the target Euclidean distance and the preset Euclidean distance matching threshold cannot be compared directly, and the matching result may be determined by determining whether the second encrypted data $g^{b \sum_1^n (x_i-y_i)^2}$ is in the matched data set

$\{g^{b \times 0}, g^{b \times 1}, g^{b \times 2}, \dots, g^{b \times \theta^2}\}$. $g^{b \sum_1^n (x_i - y_i)^2}$ being in the set $\{g^{b \times 0}, g^{b \times 1}, g^{b \times 2}, \dots, g^{b \times \theta^2}\}$ indicates that $b \sum_1^n (x_i - y_i)^2 \leq b \theta^2$, i.e., indicates that $\sqrt{\sum_1^n (x_i - y_i)^2} \leq \theta$, it may be determined that the biometric vector to be matched and the sample biometric vector are successfully matched.

[00121] The above steps c5 to c12 belong to the matching process of biometrics.

[00122] In a second example, the computational operator includes a dot product operator, and the registration and matching processes of biometrics may include the following steps d1 to d12.

[00123] In step d1, the terminal device collects sample biological data and transforms the sample biological data to a sample biometric vector $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ with a vector transformation model.

[00124] In step d2, the terminal device generates a random number a as a first private key.

[00125] In step d3, the terminal device encrypts, using a generating element g and the first private key a , the sample biometric vector $Y(y_1, y_2, y_3, \dots, y_i, \dots, y_n)$ to obtain first encrypted data.

[00126] The first encrypted data may include data $ay_i g$ and SY2 in the following equation (6), or may include data $ay_i g$ and $ay_i^2 g$ in the following equation (6), $i=1, 2, \dots, n$.

$$\text{[00127]} \quad \left\{ \begin{array}{l} y'_1 = ay_1 g \\ y'_2 = ay_2 g \\ \dots \dots \\ y'_n = ay_n g \\ SY2 = a(y_1^2 g + y_2^2 g + \dots + y_n^2 g) \end{array} \right\} \quad (6)$$

[00128] In step d4, the first encrypted data is sent to and stored by the server.

[00129] The dot product operator is in the form $g \times p$, and the elliptic curve public key cryptography in the field of cryptography may be used to ensure the security of the first encrypted data. That is, in a group of elliptic curves with a generating element g , the generating element g is a certain point on the curve, and given an integer p , it is easy to calculate $g \times p = q$, but it is difficult to calculate p from g and q . The server cannot learn the first private key a , and due to the elliptic curve cryptography, the server obtains $ay_i g$, but cannot crack and obtain y_i , and thus the first encrypted data is stored in the server in an

encrypted state.

[00130] The above steps d1 to d4 belong to the registration process of biometrics.

[00131] In step d5, the terminal device collects biological data to be matched and transforms the biological data to be matched to a biometric vector to be matched $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$ with a vector transformation model.

[00132] In step d6, the server generates a random number b as a second private key.

[00133] In step d7, the server encrypts, using the second private key, the first encrypted data to obtain first intermediate encrypted data and sends the first intermediate encrypted data to the terminal device.

[00134] The first intermediate encrypted data may include $aby_i g$ in the following equation (7).

$$\text{[00135]} \quad \begin{cases} y''_1 = aby_1 g \\ y''_2 = aby_2 g \\ \dots \dots \\ y''_n = aby_n g \end{cases} \quad (7)$$

[00136] In step d8, the terminal device obtains second intermediate encrypted data according to the biometric vector to be matched $X(x_1, x_2, x_3, \dots, x_i, \dots, x_n)$, the first intermediate encrypted data, and the first private key, and sends the second intermediate encrypted data to the server.

[00137] The second intermediate encrypted data may include $-2abx_i y_i g$ and $ax_i^2 g$ in the following equation (8).

$$\text{[00138]} \quad \begin{cases} aby_1 g \times (-2x_1) = -2abx_1 y_1 g \\ aby_1 g \times (-2x_2) = -2abx_2 y_2 g \\ \dots \dots \\ aby_1 g \times (-2x_n) = -2abx_n y_n g \\ ax_1^2 g + ax_2^2 g + \dots + ax_n^2 g \end{cases} \quad (8)$$

[00139] In step d9, the server obtains third intermediate encrypted data using the second intermediate encrypted data, the first encrypted data, and the second private key b , and sends the third intermediate encrypted data to the terminal device.

[00140] The third intermediate encrypted data includes $abg \sum_1^n (x_i - y_i)^2$ in the following equation (9).

$$\text{[00141]} \quad -2abx_1 y_1 g - 2abx_2 y_2 g + \dots - 2abx_n y_n g + ab(x_1^2 g + x_2^2 g + \dots + x_n^2 g) +$$

$$ab(y_1^2g + y_2^2g + \dots + y_n^2g) = abg \sum_1^n (x_i - y_i)^2 \quad (9)$$

[00142] It should be noted that, since the terminal device is considered as an untrusted party in the biometric matching scenario, the target Euclidean distance in an encrypted state must be constructed by the server.

[00143] In step d10, the terminal device removes, using the first private key, the first private key from the third intermediate encrypted data to obtain second encrypted data, and sends the second encrypted data to the server.

[00144] The second encrypted data includes $bg \sum_1^n (x_i - y_i)^2$ in the following equation (10).

$$[00145] \quad abg \sum_1^n (x_i - y_i)^2 \times \frac{1}{a} = bg \sum_1^n (x_i - y_i)^2 \quad (10)$$

[00146] Since the terminal device cannot learn the second private key, the terminal device is unable to construct a computational operator including a Euclidean distance less than a preset Euclidean distance matching threshold, which further improves the security of data.

[00147] In step d11, the server obtains a matched data set $\{gb \times 0, gb \times 1, gb \times 2, \dots, gb \times \theta^2\}$ according to the second private key b and a preset Euclidean distance matching threshold θ .

[00148] Herein, the preset Euclidean distance matching threshold θ , as well as the previous sample biometric vector and biometric vector to be matched, may have been converted to integers by equal multiples, and thus the number of elements in this matched data set is limited.

[00149] In step d12, the server determines whether the second encrypted data $bg \sum_1^n (x_i - y_i)^2$ is in the matched data set $\{gb \times 0, gb \times 1, gb \times 2, \dots, gb \times \theta^2\}$, if yes, it is determined that the biometric vector to be matched and the sample biometric vector are successfully matched; and if no, it is determined that the biometric vector to be matched and the sample biometric vector are failed to be matched.

[00150] The target Euclidean distance is $\sqrt{\sum_1^n (x_i - y_i)^2}$, and since the second encrypted data is in an encrypted state, the target Euclidean distance and the preset Euclidean distance matching threshold cannot be compared directly, and the matching result may be determined by determining whether the second encrypted data $bg \sum_1^n (x_i - y_i)^2$ is in the matched data set $\{gb \times 0, gb \times 1, gb \times 2, \dots, gb \times \theta^2\}$. $bg \sum_1^n (x_i - y_i)^2$ being in the set $\{gb \times 0, gb \times 1, gb \times 2, \dots, gb \times \theta^2\}$ indicates that $b \sum_1^n (x_i - y_i)^2 \leq b\theta^2$, i.e., indicates that

$\sqrt{\sum_1^n (x_i - y_i)^2} \leq \theta$, it may be determined that the biometric vector to be matched and the sample biometric vector are successfully matched.

[00151] The above steps d5 to d12 belong to the matching process of biometrics.

[00152] The third aspect of the present application provides a terminal device. Fig. 6 shows a schematic structural diagram of a terminal device according to an embodiment of the third aspect of the present application, and as shown in Fig. 6, the terminal device 400 may include a first communication module 401 and a first encryption module 402.

[00153] The first communication module 401 and the first encryption module 402 may be configured to perform, based on a first private key, an acquired biometric vector to be matched, a preset generating element, a second private key, and first encrypted data, a number of interactions and processes with a server to obtain second encrypted data.

[00154] The first private key is a private key for the terminal device. The second private key is a private key for the server. The first encrypted data is pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server. A computational operator including the second private key and a target Euclidean distance is formed in the second encrypted data. The target Euclidean distance includes a Euclidean distance between the biometric vector to be matched and the sample biometric vector.

[00155] In some examples, the computational operator includes a modular exponentiation operator or a dot product operator.

[00156] The first communication module 401 may be further configured to send the second encrypted data to the server to cause the server to obtain, using the second encrypted data, the generating element, the second private key, and a preset Euclidean distance matching threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

[00157] In the embodiments of the present application, a number of interactions and processes may be performed between the terminal device and the server based on the first private key, the biometric vector to be matched, the generating element, the second private key, and the first encrypted data, the terminal device has the first private key, the biometrics to be matched, and the generating element, and the server has the second private key and the first encrypted data.

With the encryption process by the terminal device using the first private key, the encryption process by the server using the second private key, and the data interaction between the terminal device and the server, the terminal device can obtain the second encrypted data having the computational operator including the second private key and the target Euclidean distance which can characterize the Euclidean distance between the biometric vector to be matched and the sample biometric vector, the second encrypted data contains the second private key, while the terminal device cannot learn the second private key and thus cannot crack and obtain the plaintext of the biometric vector to be matched and the sample biometric vector, and similarly, the server cannot learn the first private key and thus cannot crack the first encryption private key. Moreover, the server determines the matching result for the biometric vector to be matched and the sample biometric vector according to the second encrypted data, the generating element, the second private key, and the preset Euclidean distance matching threshold, and the matching can be achieved without involving the plaintext of the biometric vector to be matched and the plaintext of the sample biometric vector, thereby reducing the security risk of the user's privacy data and improving the security of the biometric matching. Since the terminal device and the server do not store the plaintext of the biometric vector to be matched and the plaintext of the sample biometric vector, the user's control over the personal privacy data can be ensured, thereby restricting the scenario in which the personal privacy data is used, satisfying the minimized usage principle of the personal privacy data, and preventing the personal privacy data from being abused.

[00158] Moreover, in the embodiments of the present application, the biometric vector to be matched and the sample biometric vector are encrypted, the matching result is determined by the comparison of the encrypted data, the biological data to be matched and the sample biological data are of different types, and the vector transformation models that can be adopted may also be different, while in the embodiments of the present application, the similarity of the biological data is described by the similarity of the feature vectors. During the matching of biometrics in the embodiments of the present application, the process of protecting personal privacy data and the transformation processes from the biological data to be matched to the biometric vector to be matched and from the sample biological data to the sample biometric vector may be independent of each other, thereby achieving a composable and pluggable

technical solution for the vector transformation model and the biometric matching model, i.e., achieving decoupling between the vector transformation model and the biometric matching model.

[00159] In some embodiments, the first communication module 401 may be configured to receive first intermediate encrypted data sent by the server.

[00160] The first intermediate encrypted data is obtained by the server through encrypting the first encrypted data using the second private key. Computational operators including products of the first private key, the second private key, and elements in the sample biometric vector may be formed in the first intermediate encrypted data.

[00161] The first encryption module 402 may be configured to obtain second intermediate encrypted data according to the first intermediate encrypted data, the biometric vector to be matched, the generating element, and the first private key.

[00162] Computational operators including products of the first private key, the second private key, and elements in the biometric vector to be matched are formed in the second intermediate encrypted data.

[00163] The first communication module 401 and the first encryption module 402 may be configured to perform, based on the second intermediate encrypted data, the first encrypted data, the first private key, and the second private key, interactions and processes with the server, and remove the first private key from the processed data to obtain the second encrypted data.

[00164] In some examples, the second intermediate encrypted data includes first intermediate encrypted subdata and second intermediate encrypted subdata.

[00165] The first encryption module 402 may be configured to: obtain the first intermediate encrypted subdata according to the first intermediate encrypted data and the biometric vector to be matched; and obtain the second intermediate encrypted subdata according to the first private key, the generating element, and the biometric vector to be matched.

[00166] Computational operators including products of the first private key, the second private key, elements in the sample biometric vector, and elements in the biometric vector to be matched are formed in the first intermediate encrypted subdata. Computational operators including products of the first private key and elements in the biometric vector to be matched are formed in the second intermediate encrypted subdata.

[00167] In some examples, the first communication module 401 may be configured to: send the second intermediate encrypted data to the server to cause the server to obtain third intermediate encrypted data based on the second intermediate encrypted data, the first encrypted data, and the second private key; and receive the third intermediate encrypted data sent by the server.

[00168] A computational operator including a product of the first private key, the second private key, and the target Euclidean distance is formed in the third intermediate encrypted data.

[00169] The first encryption module 402 may be configured to remove, using the first private key, the first private key from the third intermediate encrypted data to obtain the second encrypted data.

[00170] In some embodiments, the matching result includes a successful match under a condition that the second encrypted data belongs to the matched data set. The matching result includes a failed match under a condition that the second encrypted data does not belong to the matched data set. Herein, a maximum value of elements in the matched data set is obtained based on the second private key and the preset Euclidean distance matching threshold.

[00171] In some examples, elements in the biometric vector to be matched, elements in the sample biometric vector, and the preset Euclidean distance matching threshold are converted to integers by equal multiples. Computational operators including products of the second private key and each of 0 to a square of the preset Euclidean distance matching threshold after being converted to an integer being formed in the matched data set.

[00172] In some examples, the second encrypted data belongs to the matched data set under a condition that values of positions in a pre-established Bloom filter lookup table corresponding to K target hash values are all 1. The second encrypted data does not belong to the matched data set under a condition that at least one of the values of the positions in the Bloom filter lookup table corresponding to the K target hash values is 0. Herein, the K target hash values are calculated based on the second encrypted data according to K hash functions, the values in the Bloom filter lookup table are calculated based on elements in the matched data set according to the K hash functions, and K is a positive integer.

[00173] In some embodiments, the terminal device 400 may further include a first acquisition module.

[00174] The first acquisition module is configured to acquire the sample biometric vector.

[00175] The first encryption module 402 may be further configured to encrypt the sample biometric vector using the generating element and the first private key to obtain the first encrypted data.

[00176] Computational operators including products of the first private key and elements in the sample biometric vector are formed in the first encrypted data.

[00177] The first communication module 401 may be further configured to send the first encrypted data to the server.

[00178] The fourth aspect of the present application provides a server. Fig. 7 shows a schematic structural diagram of a server according to an embodiment of the fourth aspect of the present application, and as shown in Fig. 7, the server 500 may include a second communication module 501, a second encryption module 502, and a matching module 503.

[00179] The second communication module 501 and the second encryption module 502 may be configured to perform, based on a second private key, first encrypted data, a first private key, a preset generating element, and a biometric vector to be matched acquired by a terminal device, a number of interactions and processes with the terminal device to cause the terminal device to obtain second encrypted data.

[00180] The first private key is a private key for the terminal device. The second private key is a private key for the server. The first encrypted data is pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server. A computational operator including the second private key and a target Euclidean distance is formed in the second encrypted data. The target Euclidean distance includes a Euclidean distance between the biometric vector to be matched and the sample biometric vector.

[00181] In some examples, the computational operator includes a modular exponentiation operator or a dot product operator.

[00182] The second communication module 501 is further configured to receive the second encrypted data sent by the terminal device.

[00183] The matching module 503 may be configured to obtain, using the second encrypted data, the second private key, the generating element, and a preset Euclidean distance matching

threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

[00184] In the embodiments of the present application, a number of interactions and processes may be performed between the server and the terminal device based on the first private key, the biometric vector to be matched, the generating element, the second private key, and the first encrypted data, the terminal device has the first private key, the biometrics to be matched, and the generating element, and the server has the second private key and the first encrypted data. With the encryption process by the terminal device using the first private key, the encryption process by the server using the second private key, and the data interaction between the terminal device and the server, the terminal device can obtain the second encrypted data having the computational operator including the second private key and the target Euclidean distance which can characterize the Euclidean distance between the biometric vector to be matched and the sample biometric vector, the second encrypted data contains the second private key, while the terminal device cannot learn the second private key and thus cannot crack and obtain the plaintext of the biometric vector to be matched and the sample biometric vector, and similarly, the server cannot learn the first private key and thus cannot crack the first encryption private key. Moreover, the server determines the matching result for the biometric vector to be matched and the sample biometric vector according to the second encrypted data, the generating element, the second private key, and the preset Euclidean distance matching threshold, and the matching can be achieved without involving the plaintext of the biometric vector to be matched and the plaintext of the sample biometric vector, thereby reducing the security risk of the user's privacy data and improving the security of the biometric matching. Since the terminal device and the server do not store the plaintext of the biometric vector to be matched and the plaintext of the sample biometric vector, the user's control over the personal privacy data can be ensured, thereby restricting the scenario in which the personal privacy data is used, satisfying the minimized usage principle of the personal privacy data, and preventing the personal privacy data from being abused.

[00185] Moreover, in the embodiments of the present application, the biometric vector to be matched and the sample biometric vector are encrypted, the matching result is determined by the comparison of the encrypted data, the biological data to be matched and the sample

biological data are of different types, and the vector transformation models that can be adopted may also be different, while in the embodiments of the present application, the similarity of the biological data is described by the similarity of the feature vectors. During the matching of biometrics in the embodiments of the present application, the process of protecting personal privacy data and the transformation processes from the biological data to be matched to the biometric vector to be matched and from the sample biological data to the sample biometric vector may be independent of each other, thereby achieving a composable and pluggable technical solution for the vector transformation model and the biometric matching model, i.e., achieving decoupling between the vector transformation model and the biometric matching model.

[00186] In some embodiments, the second encryption module 502 may be configured to encrypt the first encrypted data using the second private key to obtain first intermediate encrypted data.

[00187] Computational operators including products of the first private key, the second private key, and elements in the sample biometric vector are formed in the first intermediate encrypted data.

[00188] The second communication module 501 may be configured to send the first intermediate encrypted data to the terminal device to cause the terminal device to obtain second intermediate encrypted data according to the first intermediate encrypted data, the biometric vector to be matched, the generating element, and the first private key.

[00189] Computational operators including products of the first private key and elements in the biometric vector to be matched are formed in the second intermediate encrypted data.

[00190] The second communication module 501 and the second encryption module 502 may be configured to perform, based on the second intermediate encrypted data, the first encrypted data, the first private key, and the second private key, interactions and processes with the terminal device to cause the terminal device to remove the first private key from the processed data to obtain the second encrypted data.

[00191] In some examples, the second intermediate encrypted data includes first intermediate encrypted subdata and second intermediate encrypted subdata.

[00192] The first intermediate encrypted subdata is obtained by the terminal device according

to the first intermediate encrypted data and the biometric vector to be matched. Computational operators including products of the first private key, the second private key, elements in the sample biometric vector, and elements in the biometric vector to be matched are formed in the first intermediate encrypted subdata.

[00193] The second intermediate encrypted subdata is obtained by the terminal device according to the first private key, the generating element, and the biometric vector to be matched. Computational operators including products of the first private key and elements in the biometric vector to be matched are formed in the second intermediate encrypted subdata.

[00194] In some examples, the second communication module 501 may be configured to receive the second intermediate encrypted data sent by the terminal device.

[00195] The second encryption module 502 may be configured to obtain third intermediate encrypted data based on the second intermediate encrypted data, the first encrypted data, and the second private key.

[00196] A computational operator including a product of the first private key, the second private key, and the target Euclidean distance is formed in the third intermediate encrypted data.

[00197] The second communication module 501 may be configured to send the third intermediate encrypted data to the terminal device to cause the terminal device to remove, using the first private key, the first private key from the third intermediate encrypted data to obtain the second encrypted data.

[00198] In some embodiments, the matching module 503 may be configured to: obtain a matched data set based on the second private key, the generating element, and the preset Euclidean distance matching threshold, a maximum value of elements in the matched data set being obtained based on the second private key and the preset Euclidean distance matching threshold; determine that the matching result includes a successful match under a condition that the second encrypted data belongs to the matched data set; and determine that the matching result includes a failed match under a condition that the second encrypted data does not belong to the matched data set.

[00199] In some examples, elements in the biometric vector to be matched, elements in the sample biometric vector, and the preset Euclidean distance matching threshold are converted to integers by equal multiples.

[00200] The matching module 503 may be configured to: calculate products of the second private key and each of 0 to a square of the preset Euclidean distance matching threshold after being converted to an integer; and obtain the matched data set according to the products of the second private key and each of 0 to the square of the preset Euclidean distance matching threshold after being converted to an integer and the generating element.

[00201] In some examples, the matching module 503 may be further configured to: calculate K target hash values based on the second encrypted data according to K hash functions; determine that the second encrypted data belongs to the matched data set under a condition that values of positions in a pre-established Bloom filter lookup table corresponding to the K target hash values are all 1; and determine that the second encrypted data does not belong to the matched data set under a condition that at least one of the values of the positions in the Bloom filter lookup table corresponding to the K target hash values is 0.

[00202] Herein, the K target hash values are calculated based on the second encrypted data according to the K hash functions, the values in the Bloom filter lookup table are calculated based on elements in the matched data set according to the K hash functions, and K is a positive integer.

[00203] In some embodiments, the server 500 may further include a lookup table generation module which may be configured to: perform, using the K hash functions, calculation on each of the elements in the matched data set to obtain K hash values corresponding to the element; and map the K hash values corresponding to the element to K positions in a binary array whose values are all 0 and update values of the K positions corresponding to the element to 1, and determine the updated binary array as the Bloom filter lookup table.

[00204] The fifth aspect of the present application further provides a terminal device. Fig. 8 shows a schematic structural diagram of a terminal device according to an embodiment of the fifth aspect of the present application. As shown in Fig. 8, the terminal device 600 includes a memory 601, a processor 602, and a computer program stored on the memory 601 and executable on the processor 602.

[00205] In some examples, the above processor 602 may include a central processing unit (CPU) or a specific integrated circuit (Application Specific Integrated Circuit, ASIC), or may be configured as one or more integrated circuits to implement the embodiments of the present

application.

[00206] The memory 601 may include Read-Only Memory (ROM), Random Access Memory (RAM), magnetic disk storage medium device, optical storage medium device, flash memory device, and electrical, optical or other physical/tangible memory storage device. Thus, generally, the memory includes one or more tangible (non-transitory) computer-readable storage media (e.g., memory devices) encoded with software including computer-executable instructions, and the software, when executed (e.g., by one or more processors), is operable to perform the operations described with reference to the biometric matching method according to the embodiments of the first aspect of the present application.

[00207] The processor 602 reads executable program codes stored in the memory 601 to execute a computer program corresponding to the executable program codes, so as to achieve the biometric matching method in the above embodiments of the first aspect.

[00208] In some examples, the terminal device 600 may further include a communication interface 603 and a bus 604. Herein, as shown in Fig. 8, the memory 601, the processor 602, and the communication interface 603 are connected through the bus 604 to complete mutual communications.

[00209] The communication interface 603 is mainly configured to implement communications among various modules, apparatus, units and/or devices in the embodiments of the present application. Input devices and/or output devices may be further accessed through the communication interface 603.

[00210] The bus 604 includes hardware, software, or both, and couples the components of the terminal device 600 together. By way of example and not limitation, the bus 604 may include Accelerated Graphics Port (AGP) or other graphics buses, Enhanced Industry Standard Architecture (EISA) bus, Front Side Bus (FSB), Hyper Transport (HT) interconnection, Industry Standard Architecture (ISA) bus, infinite bandwidth interconnection, Low pin count (LPC) bus, memory bus, Micro Channel Architecture (MCA) bus, Peripheral Component Interconnect (PCI) bus, PCI-Express (PCI-E) bus, Serial Advanced Technology Attachment (SATA) bus, Video Electronics Standards Association Local Bus (VLB) bus, or other suitable buses, or a combination of two or more of them. The bus 604 may include one or more buses where appropriate. Although the embodiments of the present application describe and illustrate

particular buses, the present application contemplates any suitable bus or interconnection.

[00211] The sixth aspect of the present application further provides a server. Fig. 9 shows a schematic structural diagram of a server according to an embodiment of the sixth aspect of the present application. As shown in Fig. 9, the server 700 includes a memory 701, a processor 702, and a computer program stored on the memory 701 and executable on the processor 702.

[00212] In some examples, the above processor 702 may include a central processing unit (CPU) or a specific integrated circuit (Application Specific Integrated Circuit, ASIC), or may be configured as one or more integrated circuits to implement the embodiments of the present application.

[00213] The memory 701 may include Read-Only Memory (ROM), Random Access Memory (RAM), magnetic disk storage medium device, optical storage medium device, flash memory device, and electrical, optical or other physical/tangible memory storage device. Thus, generally, the memory includes one or more tangible (non-transitory) computer-readable storage media (e.g., memory devices) encoded with software including computer-executable instructions, and the software, when executed (e.g., by one or more processors), is operable to perform the operations described with reference to the biometric matching method according to the embodiments of the second aspect of the present application.

[00214] The processor 702 reads executable program codes stored in the memory 701 to execute a computer program corresponding to the executable program codes, so as to achieve the biometric matching method in the above embodiments of the second aspect.

[00215] In some examples, the terminal device 700 may further include a communication interface 703 and a bus 704. Herein, as shown in Fig. 9, the memory 701, the processor 702, and the communication interface 703 are connected through the bus 704 to complete mutual communications.

[00216] The communication interface 703 is mainly configured to implement communications among various modules, apparatus, units and/or devices in the embodiments of the present application. Input devices and/or output devices may be further accessed through the communication interface 703.

[00217] The bus 704 includes hardware, software, or both, and couples the components of the server 700 together. By way of example and not limitation, the bus 704 may include

Accelerated Graphics Port (AGP) or other graphics buses, Enhanced Industry Standard Architecture (EISA) bus, Front Side Bus (FSB), Hyper Transport (HT) interconnection, Industry Standard Architecture (ISA) bus, infinite bandwidth interconnection, Low pin count (LPC) bus, memory bus, Micro Channel Architecture (MCA) bus, Peripheral Component Interconnect (PCI) bus, PCI-Express (PCI-E) bus, Serial Advanced Technology Attachment (SATA) bus, Video Electronics Standards Association Local Bus (VLB) bus, or other suitable buses, or a combination of two or more of them. The bus 704 may include one or more buses where appropriate. Although the embodiments of the present application describe and illustrate particular buses, the present application contemplates any suitable bus or interconnection.

[00218] The seventh aspect of the present application provides a biometric matching system which may include the terminal device and the server in the above embodiments, in which the terminal device can execute the biometric matching method in the above embodiments of the first aspect, and the server can execute the biometric matching method in the above embodiments of the second aspect, the specific contents of which may refer to the relevant description in the above embodiments and will not be repeated herein.

[00219] The eighth aspect of the present application further provides a computer-readable storage medium storing computer program instructions thereon. The computer program instructions, when executed by a processor, can implement the biometric matching method in the above embodiments of the first aspect or the second aspect and achieve the same technical effects, which are not repeated herein to avoid redundancy. Herein, the above computer-readable storage medium may include a non-transitory computer readable storage medium, for example, Read Only Memory (ROM), Random Access Memory (RAM), magnetic disk or optical disk, etc., which is not limited herein.

[00220] The embodiments of the present application may further provide a computer program product, in which instructions in the computer program product, when executed by a processor of an electronic device, cause the electronic device to execute the biometric matching method in the embodiments of the first aspect or the second aspect and achieve the same technical effects, the specific contents of which may refer to the relevant description in the above embodiments and will not be repeated herein to avoid redundancy.

[00221] It should be noted that the various embodiments in the specification are described in

a progressive way, the same or similar parts of various embodiments can be described with reference to each other, and each of the embodiments focuses on the differences with other embodiments. For the terminal device embodiment, the server embodiment, the system embodiment, the computer-readable storage medium embodiment, and the computer program product embodiment, reference may be made to the description of the method embodiment for the related parts. The present application is not limited to the specific steps and structures described above and illustrated in the figures. Those skilled in the art can make various changes, modifications and additions, or change the order of the steps, after understanding the gist of the present application. Further, for brevity, a detailed description of known methods and technologies is omitted herein.

[00222] Various aspects of the present application are described above with reference to flowcharts and/or block diagrams of the methods, apparatus (systems) and computer program products according to the embodiments of the present application. It should be understood that each block of the flowcharts and/or block diagrams, and a combination of blocks of the flowcharts and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, a special purpose computer, or other programmable data processing apparatus to produce a machine, so that the computer program instructions can be executed by the processor of the computer or the other programmable data processing apparatus to enable the functions/actions specified in one or more blocks of the flowcharts and/or block diagrams to be implemented. Such processor may be, but is not limited to, a general purpose processor, a special purpose processors, an application specific processor, or a field programmable logic circuit. It should also be understood that each block of the block diagrams and/or flowcharts and a combination of blocks in the block diagrams and/or flowcharts may be further implemented by special purpose hardware that performs the specified functions or actions, or by a combination of the special purpose hardware and computer instructions.

[00223] Those skilled in the art would understand that all the above embodiments are illustrative and not limiting. Different technical features in different embodiments can be combined to achieve beneficial effects. Those skilled in the art would be able to understand and implement other modified embodiments of the disclosed embodiments on the basis of

studying the drawings, the description, and the claims. In the claims, the term “comprising” does not exclude other means or steps, the quantifier “one” does not exclude multiple; the terms “first” and “second” are used to indicate names and not to indicate any particular order. Any reference signs in the claims should not be construed as limiting the protection scope. Functions of several parts in the claims can be achieved by a single hardware or software module. The presence of certain technical features in different dependent claims does not mean that these technical features cannot be combined to obtain beneficial effects.

WHAT IS CLAIMED IS:

1. A biometric matching method applied to a terminal device, the method comprising:

performing, based on a first private key, an acquired biometric vector to be matched, a preset generating element, a second private key, and first encrypted data, a number of interactions and processes with a server to obtain second encrypted data, the first private key being a private key for the terminal device, the second private key being a private key for the server, the first encrypted data being pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server, a computational operator comprising the second private key and a target Euclidean distance being formed in the second encrypted data, the target Euclidean distance comprising a Euclidean distance between the biometric vector to be matched and the sample biometric vector; and

sending the second encrypted data to the server to cause the server to obtain, using the second encrypted data, the generating element, the second private key, and a preset Euclidean distance matching threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

2. The method of claim 1, wherein the performing, based on the first private key, the acquired biometric vector to be matched, the preset generating element, the second private key, and the first encrypted data, a number of interactions and processes with the server to obtain the second encrypted data comprises:

receiving first intermediate encrypted data sent by the server, the first intermediate encrypted data being obtained by the server through encrypting the first encrypted data using the second private key, computational operators comprising products of the first private key, the second private key, and elements in the sample biometric vector being formed in the first intermediate encrypted data;

obtaining second intermediate encrypted data according to the first intermediate encrypted data, the biometric vector to be matched, the generating element, and the first private key, computational operators comprising products of the first private key, the second private key,

and elements in the biometric vector to be matched being formed in the second intermediate encrypted data; and

performing, based on the second intermediate encrypted data, the first encrypted data, the first private key, and the second private key, interactions and processes with the server, and removing the first private key from the processed data to obtain the second encrypted data.

3. The method of claim 2, wherein the second intermediate encrypted data comprises first intermediate encrypted subdata and second intermediate encrypted subdata, and

the obtaining the second intermediate encrypted data according to the first intermediate encrypted data, the biometric vector to be matched, the generating element, and the first private key comprises:

obtaining the first intermediate encrypted subdata according to the first intermediate encrypted data and the biometric vector to be matched, computational operators comprising products of the first private key, the second private key, elements in the sample biometric vector, and elements in the biometric vector to be matched being formed in the first intermediate encrypted subdata; and

obtaining the second intermediate encrypted subdata according to the first private key, the generating element, and the biometric vector to be matched, computational operators comprising products of the first private key and elements in the biometric vector to be matched being formed in the second intermediate encrypted subdata.

4. The method of claim 3, wherein the performing, based on the second intermediate encrypted data, the first encrypted data, the first private key, and the second private key, interactions and processes with the server, and removing the first private key from the processed data to obtain the second encrypted data comprises:

sending the second intermediate encrypted data to the server to cause the server to obtain third intermediate encrypted data based on the second intermediate encrypted data, the first encrypted data, and the second private key, a computational operator comprising a product of the first private key, the second private key, and the target Euclidean distance being formed in the third intermediate encrypted data;

receiving the third intermediate encrypted data sent by the server; and
removing, using the first private key, the first private key from the third intermediate encrypted data to obtain the second encrypted data.

5. The method of claim 1, wherein
the matching result comprises a successful match under a condition that the second encrypted data belongs to a matched data set;
the matching result comprises a failed match under a condition that the second encrypted data does not belong to the matched data set; and
wherein a maximum value of elements in the matched data set is obtained based on the second private key and the preset Euclidean distance matching threshold.

6. The method of claim 5, wherein
elements in the biometric vector to be matched, elements in the sample biometric vector, and the preset Euclidean distance matching threshold are converted to integers by equal multiples, and
computational operators comprising products of the second private key and each of 0 to a square of the preset Euclidean distance matching threshold after being converted to an integer being formed in the matched data set.

7. The method of claim 5, wherein
the second encrypted data belongs to the matched data set under a condition that values of positions in a pre-established Bloom filter lookup table corresponding to K target hash values are all 1;
the second encrypted data does not belong to the matched data set under a condition that at least one of the values of the positions in the Bloom filter lookup table corresponding to the K target hash values is 0; and
wherein the K target hash values are calculated based on the second encrypted data according to K hash functions, the values in the Bloom filter lookup table are calculated based

on elements in the matched data set according to the K hash functions, and K is a positive integer.

8. The method of claim 1, further comprising, before the performing, based on the first private key, the acquired biometric vector to be matched, the second private key, and the first encrypted data, a number of interactions and processes with the server to obtain the second encrypted data:

acquiring the sample biometric vector;

encrypting the sample biometric vector using the generating element and the first private key to obtain the first encrypted data, computational operators comprising products of the first private key and elements in the sample biometric vector being formed in the first encrypted data; and

sending the first encrypted data to the server.

9. The method of any of claims 1 to 8, wherein the computational operator comprises a modular exponentiation operator or a dot product operator.

10. A biometric matching method applied to a server, the method comprising:

performing, based on a second private key, first encrypted data, a first private key, a preset generating element, and a biometric vector to be matched acquired by a terminal device, a number of interactions and processes with the terminal device to cause the terminal device to obtain second encrypted data, the first private key being a private key for the terminal device, the second private key being a private key for the server, the first encrypted data being pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server, a computational operator comprising the second private key and a target Euclidean distance being formed in the second encrypted data, the target Euclidean distance comprising a Euclidean distance between the biometric vector to be matched and the sample biometric vector;

receiving the second encrypted data sent by the terminal device; and

obtaining, using the second encrypted data, the second private key, the generating element, and a preset Euclidean distance matching threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

11. The method of claim 10, wherein the performing, based on the second private key, the first encrypted data, the first private key, the preset generating element, and the biometric vector to be matched acquired by the terminal device, a number of interactions and processes with the terminal device to cause the terminal device to obtain the second encrypted data comprises:

encrypting the first encrypted data using the second private key to obtain first intermediate encrypted data, computational operators comprising products of the first private key, the second private key, and elements in the sample biometric vector being formed in the first intermediate encrypted data;

sending the first intermediate encrypted data to the terminal device to cause the terminal device to obtain second intermediate encrypted data according to the first intermediate encrypted data, the biometric vector to be matched, the generating element, and the first private key, computational operators comprising products of the first private key and elements in the biometric vector to be matched being formed in the second intermediate encrypted data; and

performing, based on the second intermediate encrypted data, the first encrypted data, the first private key, and the second private key, interactions and processes with the terminal device to cause the terminal device to remove the first private key from the processed data to obtain the second encrypted data.

12. The method of claim 11, wherein the second intermediate encrypted data comprises first intermediate encrypted subdata and second intermediate encrypted subdata,

the first intermediate encrypted subdata is obtained by the terminal device according to the first intermediate encrypted data and the biometric vector to be matched, computational operators comprising products of the first private key, the second private key, elements in the sample biometric vector, and elements in the biometric vector to be matched being formed in the first intermediate encrypted subdata, and

the second intermediate encrypted subdata is obtained by the terminal device according to the first private key, the generating element, and the biometric vector to be matched, computational operators comprising products of the first private key and elements in the biometric vector to be matched being formed in the second intermediate encrypted subdata.

13. The method of claim 12, wherein the performing, based on the second intermediate encrypted data, the first encrypted data, the first private key, and the second private key, interactions and processes with the terminal device to cause the terminal device to remove the first private key from the processed data to obtain the second encrypted data comprises:

receiving the second intermediate encrypted data sent by the terminal device;

obtaining third intermediate encrypted data based on the second intermediate encrypted data, the first encrypted data, and the second private key, a computational operator comprising a product of the first private key, the second private key, and the target Euclidean distance being formed in the third intermediate encrypted data; and

sending the third intermediate encrypted data to the terminal device to cause the terminal device to remove, using the first private key, the first private key from the third intermediate encrypted data to obtain the second encrypted data.

14. The method of claim 10, wherein the obtaining, using the second encrypted data, the second private key, the generating element, and the preset Euclidean distance matching threshold, the matching result for the biometric vector to be matched and the sample biometric vector comprises:

obtaining a matched data set based on the second private key, the generating element, and the preset Euclidean distance matching threshold, a maximum value of elements in the matched data set being obtained based on the second private key and the preset Euclidean distance matching threshold;

determining that the matching result comprises a successful match under a condition that the second encrypted data belongs to the matched data set; and

determining that the matching result comprises a failed match under a condition that the second encrypted data does not belong to the matched data set.

15. The method of claim 14, wherein elements in the biometric vector to be matched, elements in the sample biometric vector, and the preset Euclidean distance matching threshold are converted to integers by equal multiples, and

the obtaining the matched data set based on the second private key, the generating element, and the preset Euclidean distance matching threshold comprises:

calculating products of the second private key and each of 0 to a square of the preset Euclidean distance matching threshold after being converted to an integer; and

obtaining the matched data set according to the products of the second private key and each of 0 to the square of the preset Euclidean distance matching threshold after being converted to an integer and the generating element.

16. The method of claim 14, further comprising:

calculating K target hash values based on the second encrypted data according to K hash functions;

determining that the second encrypted data belongs to the matched data set under a condition that values of positions in a pre-established Bloom filter lookup table corresponding to the K target hash values are all 1;

determining that the second encrypted data does not belong to the matched data set under a condition that at least one of the values of the positions in the Bloom filter lookup table corresponding to the K target hash values is 0; and

wherein the K target hash values are calculated based on the second encrypted data according to the K hash functions, the values in the Bloom filter lookup table are calculated based on elements in the matched data set according to the K hash functions, and K is a positive integer.

17. The method of claim 16, further comprising:

performing, using the K hash functions, calculation on each of the elements in the matched data set to obtain K hash values corresponding to the element; and

mapping the K hash values corresponding to the element to K positions in a binary array whose values are all 0 and updating values of the K positions corresponding to the element to 1, and determining the updated binary array as the Bloom filter lookup table.

18. The method of any of claims 10 to 17, wherein the computational operator comprises a modular exponentiation operator or a dot product operator.

19. A terminal device comprising a first communication module and a first encryption module;

the first communication module and the first encryption module being configured to perform, based on a first private key, an acquired biometric vector to be matched, a preset generating element, a second private key, and first encrypted data, a number of interactions and processes with a server to obtain second encrypted data, the first private key being a private key for the terminal device, the second private key being a private key for the server, the first encrypted data being pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server, a computational operator comprising the second private key and a target Euclidean distance being formed in the second encrypted data, the target Euclidean distance comprising a Euclidean distance between the biometric vector to be matched and the sample biometric vector; and

the first communication module being further configured to send the second encrypted data to the server to cause the server to obtain, using the second encrypted data, the generating element, the second private key, and a preset Euclidean distance matching threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

20. A server comprising a second communication module, a second encryption module, and a matching module;

the second communication module and the second encryption module being configured to perform, based on a second private key, first encrypted data, a first private key, a preset generating element, and a biometric vector to be matched acquired by a terminal device, a

number of interactions and processes with the terminal device to cause the terminal device to obtain second encrypted data, the first private key being a private key for the terminal device, the second private key being a private key for the server, the first encrypted data being pre-obtained by the terminal device through encrypting a sample biometric vector using the generating element and the first private key and sent to the server, a computational operator comprising the second private key and a target Euclidean distance being formed in the second encrypted data, the target Euclidean distance comprising a Euclidean distance between the biometric vector to be matched and the sample biometric vector;

the second communication module being further configured to receive the second encrypted data sent by the terminal device; and

the matching module being configured to obtain, using the second encrypted data, the second private key, the generating element, and a preset Euclidean distance matching threshold, a matching result for the biometric vector to be matched and the sample biometric vector.

21. A terminal device comprising: a processor and a memory storing computer program instructions; and

the processor implementing, when executing the computer program instructions, the biometric matching method of any of claims 1 to 9.

22. A server comprising: a processor and a memory storing computer program instructions; and

the processor implementing, when executing the computer program instructions, the biometric matching method of any of claims 10 to 18.

23. A biometric matching system comprising the terminal device of claim 21 and the server of claim 22.

24. A computer-readable storage medium storing computer program instructions thereon, the computer program instructions, when executed by a processor, implementing the biometric matching method of any of claims 1 to 18.