

CLAIMS

What is claimed is:

1. An information encryption method comprising:
extracting biometric information from a biological sensor to acquire biometric data;
and
encrypting to-be-encrypted information with the biometric data according to a preset encryption algorithm to form first encrypted information, the to-be-encrypted information including a key for encrypting original data, wherein the encrypting the to-be-encrypted information with the biometric data according to the preset encryption algorithm to form the first encrypted information comprises:
converting the to-be-encrypted information into a polynomial of a predetermined format, wherein the converting the to-be-encrypted information into the polynomial of the predetermined format comprises:
segmenting the to-be-encrypted information into k segments expressed by monomials $a_1*x^{(k-1)}$, $a_2*x^{(k-2)}$, . . . , a_k*x^0 from high-bit to low-bit respectively;
converting each segment of the to-be-encrypted information into a first preset data format;
using each segment of the to-be-encrypted information of the first preset data format as a respective coefficient of a monomial corresponding to a respective segment; and
constructing a polynomial $p(x)$ of the to-be-encrypted information based on monomials of the k segments based on a formula $p(x)=a_1*x^{(k-1)}$, $a_2*x^{(k-2)}$, . . . , a_k*x^0 ,
wherein:
x is a variable of the polynomial;
 $a_1, a_2, \dots, a_k$ are coefficients of the polynomial, k being a positive integer;
and
(k-1), (k-2), . . . , k are powers of the variable x,

substituting the biometric data into the polynomial for calculation to acquire a value of the polynomial, and
using a two-dimensional dataset including the biometric data and the value of the polynomial as the first encrypted information.

2. The information encryption method of claim 1, further comprising adding check code information in the to-be-encrypted information.
3. The information encryption method of claim 2, wherein the converting the to-be-encrypted information into the polynomial of the predetermined format comprises converting the to-be-encrypted information with the added check code into the polynomial of the predetermined format.
4. The information encryption method of claim 1, further comprising adding hash data in the first encrypted information.
5. A method comprising:
extracting biometric information from a biological sensor to acquire to-be-verified biometric data;
acquiring encrypted sample data stored in a sample database;
matching the sample data with the to-be-verified biometric data according to a predetermined matching rule and using sample data meeting a matching requirement as candidate sample data;
selecting N groups of data from the candidate sample data and calculating coefficients in a polynomial corresponding to the selected N groups of data, N being a preset number of groups of selected data; and
combining the coefficients of the polynomial into first decrypted information according to a predetermined sequence of combination.
6. The method of claim 5, wherein the matching the sample data with the to-be-verified biometric data according to the predetermined matching rule and using sample data meeting the matching requirement as candidate sample data comprises:

comparing whether data in the to-be-verified biometric data and data in the sample data are identical one by one; and
 using sample data with a maximum number of identical comparison data and a matching degree not less than a preset minimum matching degree as the candidate sample data.

7. The method of claim 5, wherein the matching the sample data with the to-be-verified biometric data according to the predetermined matching rule and using sample data meeting the matching requirement as candidate sample data comprises:

calculating a respective difference between respective biometric data in the sample data and respective data in the to-be-verified biometric data by using any one of following formulas:

$$m = \sum_{i=1}^n \min(|a_{i+j} - b_i|) - t \leq j \leq t;$$

$$m = \sum_{i=1}^n \min(a_{i+j} - b_i)^2 - t \leq j \leq t; \text{ or,}$$

$$m = \sum_{i=1}^n (\min(|a_{i+j} - b_i|))^2 - t \leq j \leq t,$$

wherein:

m indicates the difference between the respective biometric data in the sample data and the to-be-verified biometric data;

n indicates a number of data in the to-be-verified biometric data;

b_i indicates a ith data of the to-be-verified biometric data;

a_{i+j} indicates a (i+j)th biometric data in the sample data; and

t indicates a preset offset; and

selecting biometric data in sample data with a minimum difference from the to-be-verified biometric data and the minimum difference being not greater than a preset maximum error value as the candidate sample data.

8. The method of claim 5, further comprising converting the first decrypted information into second decrypted information according to a predetermined conversion rule.

9. The method of claim 5, further comprising performing a cyclic redundancy check on the first decrypted information.
10. The method of claim 9, further comprising:
in response to determining that the first decrypted information does not pass the cyclic redundancy check,
re-selecting N groups of data from the candidate sample data;
calculating coefficients of a polynomial corresponding to the re-selected N groups of data to acquire new decrypted information; and
performing a cyclic redundancy check on the new decrypted information.
11. The method of claim 10, further comprising determining that a result of information decryption is a failure in response to determining that none of decrypted information corresponding to all of N groups of data in L pieces of data of the candidate sample data passes the cyclic redundancy check.
12. An information encryption apparatus comprising:
an information receiving module that acquires to-be-encrypted information, the to-be-encrypted information including a key for encrypting original data;
a biometric information module that extracts biometric information from a biological sensor to acquire biometric data; and
an encryption module that encrypts the to-be-encrypted information with the biometric data according to a preset encryption algorithm to form first encrypted information, wherein the encryption module comprises:
an information conversion module that converts the to-be-encrypted information into a polynomial of a predetermined format, wherein the information conversion module comprises:
a segmenting module that segments the to-be-encrypted information into k segments, and expresses the to-be-encrypted information after the segmentation by monomials $a_1 \cdot x^{(k-1)}$, $a_2 \cdot x^{(k-2)}$, $a_k \cdot x^0$ from high-bit to low-bit respectively,
a first preset data module that converts each segment of the to-be-encrypted information into a first preset data format and uses each segment of the to-

be-encrypted information of the first preset data format as a respective coefficient of a monomial corresponding to a respective segment, a polynomial construction module that constructs a polynomial $p(x)$ of the information based on monomials of the k segments based on a formula $p(x)=a_1*x^{(k-1)}, a_2*x^{(k-2)}, \dots, a_k*x^0$, wherein:
 x is a variable of the polynomial;
 $a_1, a_2, \dots, a_k$ are coefficients of the polynomial, k being a positive integer;
and
 $(k-1), (k-2), \dots, k$ are powers of the variable x , and
a mapping module that substitutes the biometric data into the polynomial for calculation to acquire a value of the polynomial, and forms the first encrypted information based on two-dimensional data including the biometric data and the value of the polynomial.

13. The information encryption apparatus of claim 12, further comprising a check code addition module that adds check code information in the to-be-encrypted information.

14. The information encryption apparatus of claim 13, wherein the information conversion module converts the to-be-encrypted information with the added check code into the polynomial of the predetermined format.

15. The information encryption apparatus of claim 12, further comprising a hash data module that adds hash data in the first encrypted information.

16. The information encryption apparatus of claim 12, wherein the biometric information includes biometric information of a fingerprint or a retina.