Computers, Materials & Continua CMC, vol.61, no.2, pp.727-738, 2019

Achieving Privacy-Preserving Iris Identification Via El Gamal

Yong Ding[1], Lei Tian[1], Bo Han[2], Huiyong Wang[2, *], Yujue Wang[1] and James Xi Zheng[3]

Abstract: Currently, many biometric systems maintain the user's biometrics and templates in plaintext format, which brings great privacy risk to uses' biometric information. Biometrics are unique and almost unchangeable, which means it is a great concern for users on whether their biometric information would be leaked. To address this issue, this paper proposes a confidential comparison algorithm for iris feature vectors with masks, and develops a privacy-preserving iris verification scheme based on the El Gamal encryption scheme. In our scheme, the multiplicative homomorphism of encrypted features is used to compare of iris features and their mask information. Also, this paper improves the Hamming distance of iris features, which makes the similarity matching work better than existing ones. Experimental results confirm the practicality of our proposed schemes in real world applications, that is, for the iris feature vectors and masks of 2048 bits, nearly 12 comparisons can be performed per second.

Keywords: Homomorphic encryption, template matching, Hamming distance.

1 Introduction

With the rapid development of the Internet and e-commerce, more and more scenarios in daily life require identity authentication for users, for example, services provided in airports and banks, and applications on mobile phones, ATMs and online financial services. With traditional identity authentication methods, passwords are easy to be forgotten or lost, and 'mobile phone number + verification code' in the identity authentication approach can be easily intercepted. Therefore, some biometric identification technologies have been developed [Cimato, Gamassi and Piuri (2009)].

However, most of existing biometric identification technologies perform feature comparisons in the plaintext format. Once the biometric information is stolen by hackers or internal personals, it may cause serious consequences of large-scale user private information leakage. In fact, the risk of user's biometric information leakage is no less than losing traditional identification media, such as ID cards. Although some studies have been focused on addressing the security and privacy issues of biometric, existing biometric

[1] Guangxi Key Laboratory of Cryptography and Information Security, School of Computer and Information Security, Guilin University of Electronic Technology, Guilin, 541004, China.

[2] School of Mathematics and Computer Science, Guilin University of Electronic Technology, Guilin, 541004, China.

[3] Software Engineering Department of Computing, Macquarie University, Sydney, NSW 2109 Australia.

[*] Corresponding Author: Huiyong Wang. Email: why6082015@gmail.com.

systems may confront more and more difficulties in protecting biometric information against hardware attacks and system security cracking technologies [Liu, Wang, Chaudhry et al. (2018)].

In existing works, it is difficult to give accurate definitions on the security and privacy protection on biometric information in biometric systems. Ratha et al. summarized eight attack points on the inter-module channel in biometric systems [Ratha, Connell, Bolle et al. (2006)]. These attacks can be divided into four types according to the locations of attacks [Parbhakar, Pankanti and Jain (2003); Menaria and Jain (2017)], that is, physical layer attacks, transport attacks against feature and template databases, storage attacks against features and template databases, and attacks on software modules.

There are some typical patterns for the above mentioned attacks:

(1) Forged biometric attack: The attacker may use fake biometric features, for example, plastic fingerprints, to access the system;

(2) Replay attack: The attacker may steal biological information from the transmission channel, and use them in completing identification;

(3) Coverage feature extractor: The attacker may replace the processing results of the feature extractor with custom templates;

(4) Forge the feature vector: The transmitted data between the feature extractor and matcher may be replaced by fake features;

(5) Rewrite the matcher: Make the matcher output the results according to the attacker's expectation;

(6) Change the template: Some templates may be modified, deleted or added to the database;

(7) Attack channel: The transmission information between the database and matcher may be changed using different templates;

(8) Rewrite the final decision: The attacker may modify or disturb traditional binary biometric with success rate of more than 50%.

Although the first type of attacks can be resisted by employing the living body detection technology, this technology is still imperfect. Also, some methods can resist the attacks in identifying the interior of system, for example, enhance the security of the channel, encrypt the data to prevent from theft, add time-stamps to the data to prevent from replay attacks, and install anti-trojan and virus security software for the template database to ensure that the database cannot be tampered with.

Unauthorized access to biometric templates is generally considered to be the greatest threat to the user's data security. Therefore, the protection of biometric templates becomes a key issue, where biometric template protection schemes should satisfy the following properties:

(1) Renewability: It should be possible to revoke the leaked biometric templates and generate new biometric templates based on the same biometric data;

(2) Diversity: The regenerated biometric templates should not match with the revoked template from the same biometric;

(3) Security: It should be impossible to obtain raw biometric data from biometric templates, or at least the computation should be difficult;

(4) The template storage scheme should not cause significant decrease in the biometric recognition rate, such as the error rejection rate and the error acceptance rate.

Due to some factors such as the collection environment, the biometric characteristics of the same person will be slightly different in each acquisition. Thus, researchers have proposed a variety of methods for biometric template protection, which can be divided into the following categories:

(1) Template protection method based on feature transformation [Nanni and Lumini (2008)]. This method requires a function to transform the biometric or template and match it in the transform domain. The transformation function should be invertible or irreversible. Note that a method based on reversible transformation will result in a lower error reception rate, however, when the parameters of transformation function are leaked, user templates would not safe due to the reversibility of the transformation. On the contrary, for irreversible transformation, even if the transformed parameters are leaked, it is difficult to deduce too much information about biometric templates.

(2) Template protection method based on biometric encryption. This method stores the encrypted biometric data as templates. According to different key sources, this category of template protection methods can be further divided into two types, that is, key generation methods and key binding methods.

(3) Template protection method based on secret sharing. The idea of secret sharing is to split the secrets in an appropriate way, where shares are managed by different participants, and only participants in the authorized sets can collaborate to recover the secret message. Thus, if the collected biometrics (plaintext or ciphertext) can be split and stored in multiple servers, the data leakage issue in the single server scenario can be effectively avoided, and the system can be disaster-tolerant.

(4) Template protection method based on homomorphic encryption [Brakerski and Vaikuntanathan (2014)]. With this method, the obtained iris feature template is protected in ciphertext format by a homomorphic encryption scheme.

Our contributions

To address the above mentioned issues, this paper proposes a privacy-preserving iris identification scheme. The iris feature template is processed as an image, then the output is treated as a binary vector for random number substitution to obtain a set of two-dimensional vectors. These vectors are further dealt with the El Gamal encryption scheme to obtain the replaced iris information.

The experiment uses the iris feature templates in CASIA database (https://download.csdn.net). An improved non-secure alignment algorithm was used to encrypt the iris feature template, which matched through similarity calculation. The simulation of iris recognition confirms that the performance of our scheme outperforms the traditional method. Therefore, it is practical to be deployed in small-scale iris recognition applications.

2 Preliminaries

2.1 Homomorphic encryption

Homomorphic encryption was proposed by Rivest et al. [Rivest, Adleman and Dertouzos (1978)]. Suppose the domain of a function is set X, the value field is Y, and the corresponding law is f. If for $x_1, x_2 \in \{X\}$, $f(x_1 \oplus x_2) = f(x_1) \oplus f(x_2)$ holds, then the law f satisfies the homomorphism. In cryptography, it can be expressed as follows: If the encryption algorithm E satisfies $E(m_1 \oplus m_2) = E(m_1) \oplus E(m_2)$, then it is called adding homomorphism; if E satisfies $E(m_1 \otimes m_2) = E(m_1) \otimes E(m_2)$, then it is called multiplicative homomorphism. A semi-homomorphic encryption scheme only satisfies either addition homomorphism or multiplication homomorphism, whereas both are satisfied in a fully encryption scheme. Note that the El Gamal scheme [Xie (2014)] only satisfies the multiplicative homomorphism, which means it is a semi-homomorphic scheme.

2.2 El Gamal encryption algorithm

The El Gamal scheme [Elgamal (1985)] can be used to encrypt each element of a matrix after permutation. Let G=<a>=$\{\ldots, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, a^3, \ldots\}$ be a cyclic group. First select a large prime number p such that $p-1$ has a large prime factor. Then, select the primitive a of the modulo p, publish p and a, randomly select an integer d $(2 \le d \le p-2)$ as the private key, and calculate $y = a\text{^}d\ (mod\ p)$ as the public key. For encryption, randomly select an integer $k(2 \le k \le p-2)$, and calculate the ciphertext$c_1 = a\text{^}k\ (mod\ p)$ and $c_2 = y\text{^}k * m\ (mod\ p)$.

2.3 Template matching

Template matching is usually performed according to their similarity [Zhang (2001)]. There are three commonly used methods for calculating similarity. In the following, suppose x_i and y_i represent two-dimensional vectors.

Euclidean distance: The matching formula is defined as $L(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$. Although Euclidean distance calculation is simple and efficient, it has obvious disadvantages, for example, it treats different attributes in the processing object equally and may sometimes fails to meet actual needs.

Block distance: The matching formula is defined as $L(x,y) = \sum_{i=1}^{n}|x_i - y_i|$. This method is generally applied to the distance between two points in the plane, which is simpler than the Euclidean distance's calculation. However, it cannot be applied to binary strings.

Hamming distance: The matching formula is defined as $HD = \sum_{i=1}^{n} x_i \oplus y_i$. Hamming distance is generally applied to the fields of information theory, coding theory, cryptography, etc., and it is applicable to binary strings. Due to its preferable properties, this method is employed in the template matching algorithm in this paper.

Evaluation indicators: The evaluation index in the commonly used iris recognition system [Ma, Tan and Wang (2004)] reflects the rejection rate. The false rejection rate, also known as the rejection rate, represents the probability that a legitimate user is considered as an illegal user. The false acceptance rate, also known as the false positive rate, indicates the probability that an illegal user is considered as a legitimate user. The rejection rate can be

divided into error acceptance rate (FAR), error rejection rate (FRR), error rate (EER), and overall error rate (TER), where TER is the sum of FAR and FRR. The equal error rate means that FRR and FAR are the same after the wait threshold is determined. By taking different thresholds, FRR will be different from FAR, and usually their variation is inversely proportional.

2.4 Iris recognition general process

The iris recognition process mainly includes image collection, image processing, feature encoding, feature matching, and conclusion. In this paper, we mainly focus on the feature coding and the feature matching procedures. To guarantee the privacy, the El Gamal scheme is used to encrypt the encoded iris information, and then the improved Hamming distance is used for feature matching in feature matching [Lv, Lv and Zhao (2017)]. Note that a threshold should be set at the initiation phase. If the Hamming distance is less than the pre-defined threshold, the recognition passes, otherwise it fails. The general process of iris recognition is shown in Fig. 1.

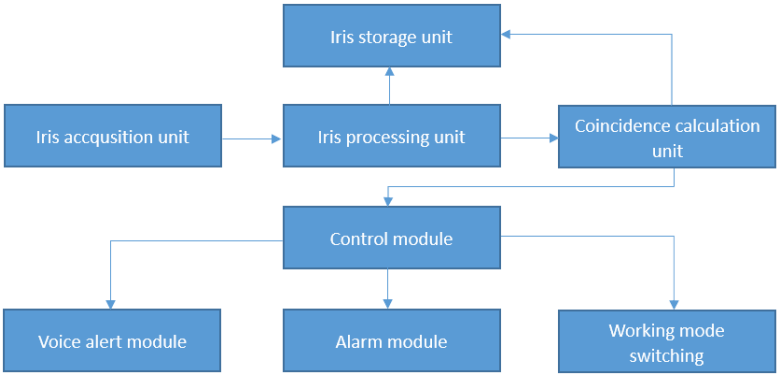

Figure 1: General process of Iris recognition

3 Main technical operation of iris recognition

3.1 Image Preprocessing

The pre-preocessing of iris images [Ji (2016); Marina and Paolo (2011); Liu, Zhang, Li et al. (2016)] can be divided into the following steps:

(1) Extracting iris region: For the input image, first convert into a grayscale one, then employ the Canny operator to perform edge detection to obtain the inner edge of Iris, and followed by a Hough transform for detecting the outer edge of iris.

(2) Coordinate transformation: Note that the iris area extracted in Step (1) is ring-shaped, whereas the general image is rectangular. Thus, to facilitate the subsequent procedures, the obtained iris image is subjected to polar coordinate transformation and satisfies $r = \sqrt{x^2 + y^2}$ and $\theta = arctan\frac{y}{x}$. In this way, the ring-shaped iris area is converted into a rectangle one.

(3) Normalization: Since the texture information of iris is affected by eyelids, eyelashes,

etc., the closer to the outer edge, the more susceptible it is to interference. Therefore, the part close to the inner edge of iris is selected as the image containing the iris texture information. The obtained image contains both rich iris texture information and the amount of calculation. Finally, the rectangular area is normalized to 250×20 pixels.

3.2 Iris feature extraction

The iris image obtained above is subjected to feature extraction using a Gabor filter [Panchal and Samanta (2016); Li, Sun and Tan (2016)]. The iris feature is in fact the texture information. The difference between the iris signals is caused by different texture information. Therefore, the iris signal is the description of texture information, and the Gabor filter is the core algorithm proposed by Duangrna [Daugman (2003)] to extract the iris feature. In this paper, this classical algorithm is employed to extract iris features using Gabor filtering.

3.3 Privacy-preserving comparison

Since the iris feature is a binary vector after encoding, the Hamming distance is employed in performing template matching. The template matching method described above is directly operated on the iris texture information, which would result in information leakage. We propose an improved method of template matching.

The extracted iris feature template is denoted by $X(m,n)$, and the template to be matched is $Y(m,n)$, where m,n represent the row and column of the template matrix, respectively. In the iris feature extraction process, there are interference factors such as eyelids and eyelashes. These points are used as interference points when extracting features and encoding. When the iris is segmented, the pixels of these interference points are marked and generated. Iris feature template has the same size of interference template, they are written as $MX(m,n)$ and $MY(m,n)$. The mask is generated to remove interference points and improve the matching degree. If the extracted feature points are interference points, the feature points of $MX(m,n)$and $MY(m,n)$ are recorded as 1 at the corresponding positions, otherwise they are recorded as 0. In this paper, an improved Hamming distance formula is defined as follows:

$$HD = \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{X(i,j)\oplus Y(i,j)\wedge MX(i,j)\wedge MY(i,j)}{|MX(i,j)\wedge MY(i,j)|} \quad (1)$$

4 Our method

Since the randomness of information encryption will affect the quality of encryption, our approach can be divided into the following three schemes with different randomness.

4.1 Scheme 1

(1) Mapping

Randomly take two fixed prime numbers a,b, and use them to transform the obtained iris feature templates $X(i,j)$ and $Y(i,j)$ as follows:

$$X(i,j) = \begin{cases} a, X(i,j) = 1 \\ b, X(i,j) = 0 \end{cases} \quad (2)$$

$$Y(i,j) = \begin{cases} a, X(i,j) = 1 \\ b, X(i,j) = 0 \end{cases} \quad (3)$$

(2) Encryption

The vector information obtained in Step (1) is encrypted by using the encryption algorithm described in Section 2.2, where m represents a and b in Step (1), and the encrypted X, Y, MX and MY are represented as $E(X)$, $E(Y)$, $E(MX)$ and $E(MY)$, respectively.

(3) Matching

Perform similarity analysis using the secret comparison algorithm described in Section 3.4. Replace X, Y, MX and MY in the formula by $E(X)$, $E(Y)$, $E(MX)$ and $E(MY)$, respectively. That is, the original formula is converted to the following:

$$HD = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{E(X(i,j)) \oplus E(Y(i,j)) \wedge E(MX(i,j)) \wedge E(MY(i,j))}{|E(MX(i,j)) \wedge E(MY(i,j))|} \quad (4)$$

By calculating the relationship between the Hamming distance value and the pre-defined threshold τ, if HD < τ, it succeeds to pass, otherwise it fails.

4.2 Scheme 2

The difference between Scheme 2 and Scheme 1 is that the substitution formula is changed in Step (1). Specifically, for each element $X(i,j)$, two prime numbers a_i, b_i are randomly chosen, which are used to transform the obtained iris feature templates $X(i,j)$ and $Y(i,j)$ as follows:

$$X(i,j) = \begin{cases} a_i, X(i,j) = 1 \\ b_i, X(i,j) = 0 \end{cases} \quad (5)$$

$$Y(i,j) = \begin{cases} a_i, X(i,j) = 1 \\ b_i, X(i,j) = 0 \end{cases} \quad (6)$$

The other two steps are the same as in Scheme 1. In fact, by adding more randomness on the basis of Scheme 1, it could provide more security for the iris feature template.

4.3 Scheme 3

This scheme introduces the randomness to the replacement, in this way to improve the security of Scheme 2. The following changes are made to Scheme 2. For each element $X(i,j)$, two prime numbers a_i, b_i are randomly chosen, a prime number p is picked, and compute the iris feature template $X(i,j)$ and $Y(i,j)$ as follows:

$$X(i,j) = \begin{cases} pa_i, X(i,j) = 1 \\ b_i, X(i,j) = 0 \end{cases} \quad (7)$$

$$Y(i,j) = \begin{cases} pa_i, X(i,j) = 1 \\ b_i, X(i,j) = 0 \end{cases} \quad (8)$$

The other steps are exactly the same as in Scheme 1.

4.4 Correctness analysis

(1) With the El Gamal scheme, the ciphertext length is twice the plaintext length. Note that

$X(i,j)$ is changed to $X(i,2j)$. For example, given $X = \begin{pmatrix} a & b \\ a & b \end{pmatrix}$, it is changed to $X = \begin{pmatrix} c_{11} & c'_{11} & c_{12} & c'_{12} \\ c_{21} & c'_{21} & c_{22} & c'_{22} \end{pmatrix}$ by following the encrypt algorithm. Let the corresponding elements of $E(X)$ and $E(Y)$ be c_1, c'_1 and c_2, c'_2, and the corresponding elements of $E(MX)$ and $E(MY)$ be mc_1, mc'_1 and mc_2, mc'_2. $c_1 = \mathrm{a}_1\text{^}k_1\ (mod\ p)$, $c_2 = \mathrm{a}_2\text{^}k_2\ (mod\ p)$, $c'_1 = y_1\text{^}k_1 * m_1\ (mod\ p)$, $c'_2 = y_2\text{^}k_2 * m_2\ (mod\ p)$, $mc_1 = \mathrm{a}_3\text{^}k_3\ (mod\ p)$, $mc_2 = \mathrm{a}_4\text{^}k_4\ (mod\ p)$, $mc'_1 = y_3\text{^}k_3 * m_3\ (mod\ p)$, $mc'_2 = y_4\text{^}k_4 * m_4\ (mod\ p)$, it can be seen that m_1, m_2, m_3, m_4 are replaced with a and b. Obviously, m_1, m_2, m_3, m_4 belong to the set $A = \{a^2, b^2, ab\}$. Consider the following formula

$$HD = \sum_{i=1}^{m}\sum_{j=1}^{n} \frac{E(X(i,j)) \oplus E(Y(i,j)) \wedge E(MX(i,j)) \wedge E(MY(i,j))}{|E(MX(i,j)) \wedge E(MY(i,j))|} \tag{9}$$

where $\oplus$ and $\wedge$ denote exclusive OR operation and AND operation, respectively.

Scheme 1

(1) For the operation $\oplus$: $E\big(X(i,j)\big) * E\big(Y(i,j)\big)\ mod\ (ab)$, $c_1 * c_2\ mod\ p = \mathrm{a}_1\text{^}k_1\ (mod\ p) * \mathrm{a}_2\text{^}k_2\ (mod\ p) = a_1\text{^}k_1 * a_2\text{^}k_2\ mod\ p$, $c'_1 * c'_2\ mod\ p = y_1\text{^}k_1 * m_1\ (mod\ p) * y_2\text{^}k_2 * m_2\ (mod\ p)$:

Since m_1 and m_2 are elements in the A, the exclusive OR operation is different for the corresponding positional elements. Thus, when $E\big(X(i,j)\big) * E\big(Y(i,j)\big)\ mod\ (ab) = 0$, it means that m_1 and m_2 are different.

(2) For the $\wedge$ operation: $E(MX(i,j)) * E\big(MY(i,j)\big) mod\ (b^2)$:

In binary operations, $\wedge$ indicates that it outputs 1 if all elements in the vector are all 1; otherwise, it outputs 0. In contrast, the permutation method of Scheme 1 is conducted on b with the $\wedge$ operation. Thus, $mc_1 * mc_2 = \mathrm{a}_3\text{^}k_3\ (mod\ p) * \mathrm{a}_4\text{^}k_4\ (mod\ p) = \mathrm{a}_3\text{^}k_3 * \mathrm{a}_4\text{^}k_4\ (mod\ p)$, $mc'_1 * mc'_2 = y_3\text{^}k_3 * m_3\ (mod\ p) * y_4\text{^}k_4 * m_4\ (mod\ p) = y_3\text{^}k_3 * y_4\text{^}k_4 * m_3 * m_4\ (mod\ p)$.

Since m_3 and m_4 are also the elements in set A, when $E(MX(i,j)) * E\big(MY(i,j)\big)\ mod\ (b^2)$ is stated, both m_1 and m_2 are b at the time of replacement.

Similarly, we have the following correctness analysis of Scheme 2 and Scheme 3.

Scheme 2

For the operation $\oplus$: $E\big(X(i,j)\big) * E\big(Y(i,j)\big)\ mod\ (a_i b_i)$, when the original is equal to 0, m_1 is different from m_2. For the operation $\wedge$: $E(MX(i,j)) * E\big(MY(i,j)\big)\ mod\ (b_i^2)$, when the original is equal to 0, both m_1 and m_2 are b at the time of replacement.

Scheme 3

For the operation $\oplus$: $E\big(X(i,j)\big) * E\big(Y(i,j)\big)\ mod\ (pa_i b_i)$, when the original is equal to 0, m_1 is different from m_2. For the operation $\wedge$: $E(MX(i,j)) * E\big(MY(i,j)\big)\ mod\ (b_i^2)$, when the original is equal to 0, both m_1 and m_2 are b at the time of replacement.

5 Experimental analysis

Our experiments are conducted on WIN7 Ultimate operating system using the C

programming language and MATLAB, where the CASIA iris database is used. Since Scheme 2 and Scheme 3 are developed by introducing more randomness to Scheme 1, they can enhance the security of iris information with Scheme 1. The more randomness, the lower computational efficiency. Therefore, we focus on analyzing the practicality of Scheme 3 with the best efficiency. As shown in Tab. 1 and Tab. 2, the iris identification achieves optimal effect when the Hamming distance HD=0.3. Thus, in the experiment, the threshold is taken as 0.3. Tab. 1 and Tab. 2 show the relationship between the threshold and FRR, FAR for the plaintext state and the ciphertext state, respectively.

Table 1: Error rejection rate *vs.* error acceptance rate (plain-text)

Hamming distance HD (Threshold)	FAR (%)	FRR (%)
0.10	0.000	99.174
0.15	0.000	82.645
0.20	0.000	42.149
0.25	0.000	8.264
0.30	0.008	0.283
0.35	9.917	0.000
0.40	91.973	0.000
0.50	99.669	0.000

Table 2: Error rejection rate *vs.* error acceptance rate (ciphertext)

Hamming distance HD (Threshold)	FAR (%)	FRR (%)
0.10	0.000	99.256
0.15	0.000	82.727
0.20	0.000	42.231
0.25	0.000	8.264
0.30	0.008	0.331
0.35	16.529	0.000
0.40	91.983	0.000
0.50	99.669	0.000

According to the experiments, the selected threshold value directly affects the running timings of our Schemes. Fig. 2 and Fig. 3 demonstrate the running timing of our scheme under different thresholds for the plaintext state and the ciphertext state, respectively. From these figures, it is easy to see that when the threshold is 0.3, the proposed scheme takes nearly the most computing time. However, this threshold implies nearly the optimal recognition effect. When the length of iris feature vectors and masks is 2048 bits, the proposed privacy-preserving comparison algorithm can complete 12 iris comparisons per

second. Thus, our solution is practical and secure when applied in small-scale iris recognition scenarios.

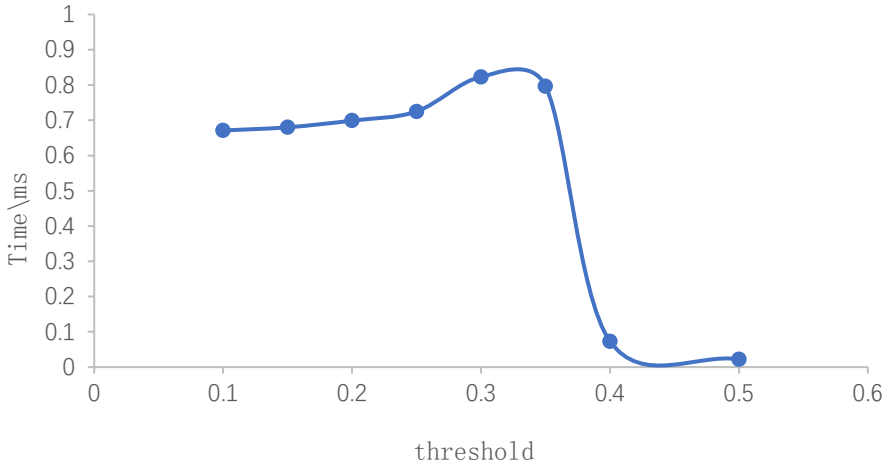

Figure 2: Identification efficiency for plaintext case

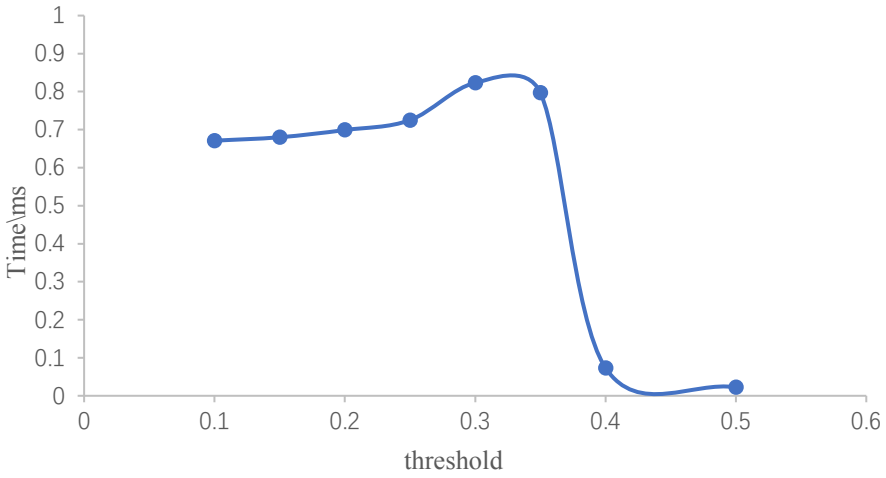

Figure 3: Identification efficiency for ciphertext case

6 Conclusion

In this paper, a privacy-preserving iris feature vector comparison algorithm with mask is designed, where the iris feature information and the mask are encrypted by the El Gamal scheme. This paper also proposes an improved Hamming distance formula. With the multiplicative homomorphism of El Gamal scheme, the comparison of iris feature and

mask information can be conducted in ciphertext format without leaking their privacy. Extensive experimental results demonstrate that the proposed scheme achieves preferable recognition effects and enjoys high efficiency.

Acknowledgements: This work was partially supported by the National Natural Science Foundation of China (Grant Nos. 61772150, 61862012), the National Cryptography Development Fund of China under project MMJJ20170217, the Guangxi Key R&D Fund under project AB17195025, the Guangxi Natural Science Foundation under grant 2018GXNSFAA281232, the open project of Guangxi Key Laboratory of Cryptography and Information Security (Grant Nos. GCIS201622, GCIS201702), and the GUET Excellent Graduate Thesis Program (16YJPYSS23).

References

Brakerski, Z.; Vaikuntanathan, V. (2014): Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on Computing*, vol. 43, no. 2, pp. 97-106.

Cimato, S.; Gamassi, M.; Piuri, V.; Sassi, R.; Scotti, F. (2009): A multi-biometric verification system for the privacy protection of iris templates. *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems*, vol. 57, pp. 227-234.

Daugman, J. (2003): The importance of being random statistical principles of recognition. *Pattem recognition*, vol. 36, no. 2, pp. 279-291.

Elgamal, T. (1985): A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472.

Ji, X. (2016): *Research on Key Issues in Iris Recognition Algorithm (Ph.D. Thesis)*. Beijing Jiaotong University, China.

Li, H.; Sun, Z.; Tan, T. (2016): Development and trend of iris recognition technology. *Information Security Research*, vol. 1, no. 1, pp. 40-43.

Liu, P.; Wang, X.; Chaudhry, S. R.; Javeed, K.; Ma, Y. et al. (2018): Secure video streaming with lightweight cipher PRESENT in a SDN testbed. *Computers, Materials & Continua*, vol. 57, no. 3, pp. 353-363.

Liu, N.; Zhang, M.; Li, H.; Sun, Z; Tan, T. (2016): DeepIris: learning pairwise filter bank for heterogeneous iris verification. *Pattern Recognition Letters*, vol. 82, no. 2, pp. 154-161.

Lv, K.; Lv, X.; Zhao, W. (2017): Study on iris pretreatment and texture feature extraction method. *Modern Electronic Technology*, vol. 40, no. 16, pp. 112-116.

Ma, L.; Tan, T.; Wang, Y.; Zhang, D. X. (2004): Efficient iris recognition by characterizing key local variations. *IEEE Transactions on Image Processing*, vol. 13, no. 6, pp. 739-750.

Marina, B.; Paolo, G. (2011): Efficient protocols for iris and fingerprint identification. *Computer Security-ESORICS*, vol. 6879, no. 3, pp. 190-209.

Menaria, L.; Jain, K. (2017): A survey on biometric template protection. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 2, no. 2, pp. 995-999.

Nanni, L.; Lumini, A. (2008): Random subspace for an improved biohashing for face authentication. *Pattern Recognition Letters*, vol. 29, no. 3, pp. 295-300.

Panchal, G.; Samanta, D. (2016): Comparable features and same cryptography key generation using biometric fingerprint image. *International Conference on Advances in Electrical Electronics Information Communication and Bio Informatics*, pp. 691-695.

Prabhakar, S.; Pankanti, S.; Jain, A. K. (2003): Biometric recognition: security and privacy concerns. *IEEE Security & Privacy*, vol. 1, no. 2, pp. 33-42.

Ratha, N.; Connell, J.; Bolle, R. M.; Chikkerur, S. (2006): Cancelable biometrics: a case study in fingerprints.*18th International Conference on Pattern Recognition*, vol. 4, no. 4, pp. 370-373.

Rivest, R. L.; Adleman, L.; Dertouzos, M. L. (1978): On data banks and privacy homomorphisms. *Foundations of Secure Computation*, vol. 4, no. 11, pp. 169-179.

Xie, X. (2014): *Homomorphic Calculation of Cryptographic Algorithm (Ph.D. Thesis)*. Xidian University.

Zhang, H. (2001): Text similarity calculation based on Hamming distance. *Computer Engineering and Applications*, vol. 37, no. 19, pp. 21-22.