International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.315-330
http://dx.doi.org/10.14257/ijsia.2016.10.6.30

A Novel Face Template Protection Algorithm Based on the Fusion of Chaos Theory and RSA Encryption

Liu Yunan[1], Zhao Fudong[2], Xu Yanli[3] and Cao Yu[2*]

1.School of Foreign Languages, Harbin University of Science and Technology, Harbin, 150080, China
2.School of Automation, Harbin University of Science and Technology, Harbin, 150080, China
3.School of Foreign Languages, Northeast Forestry University, Harbin, 150040, China
cyhit@163.com

Abstract

In the face recognition system, the protection of the facial feature template has already become the most important part. In view of that the current protection methods cannot meet the security and the matching rate simultaneously, a hybrid encryption algorithm was proposed in this paper fusing chaotic encryption and RSA encryption to solve this problem. After the preprocessing to the ORL face database, the feature template was extracted by $2D^2$LDA and PCA in the non-transformation domain. Then we applied the scrambling encryption and RSA encryption to obtain the final security template. At last, a system with the nearest neighbor classifier and Euclidean distance was used for the matching verification. The experimental results showed that this hybrid encryption method was feasible, effective and easy transplantation with no matching rate reduction.

Keywords: *facial feature; encryption; Chaos theory; RSA*

1. Introduction

Biometric identification technology, especially based on the fingerprint identification technology has been widely applied in real life and has brought great convenience for us [1-3]. Compared with the mature fingerprint technology face feature research can also achieve high recognition effect [4-6]. However, the security problem has become the biggest obstacle to the application of face recognition technology.

A biometric encryption algorithm can be convinced satisfy security, cancelability and discriminability [7]. In order to achieve the functions above, the mature fingerprint feature encryption algorithms were applied into face feature in transformation direction and non-transformation direction. In the transform domain, help data theory and biometric hash were invented to ensure the recognition accuracy. In the study of the past Wang Q and Huang W got the safe template based on the Fuzzy Commitment Scheme [8, 9]. They quantified the face feature template after feature extraction, and then do XOR with random error correcting code to complete the requirements. But the calculation process is a little computation-expensive and has lack of a detail analysis about the security. Yi C. Feng and Pong C. Yuen improved the recognition results by classifying the facial features accurately [10]. In their study, a random projection was adopt in the first step to provide cancelability. In the next core step the authors put the database which contains C classes of training samples into two classes, and then determined a cluster of corresponding distinguishing points to separate the two classes. After calculate c sets of

* Corresponding Author

ISSN: 1738-9976 IJSIA

clusters, different face feature templates for matching are obtained by hash threshold. This method makes the performance better than non-encryption. Wu Y. Chen proposed a Fuzzy Cyclic Random Mapping method which use the previous cycle key created the next dimensionality reduction mapping matrix [11]. After multiple cycles, a security template is obtained by applying a hash threshold. This method guarantees that the matching rate will not be reduced and a very good performance can be achieved in the case of less training samples. But, the application of hash algorithm can only be used after define the secondary characteristics. And makes the algorithm complex and require large numbers of secret keys to be stored. Therefore, some image encryption algorithms in the non-transform domain are also referenced to the face feature protection. Divya James and Mintu Philip combines the chaos theory which is outstanding in the image encryption with visual cryptography concepts, decompose the input image into two encrypted independent public host image and only can be decrypted after collected both of them [12]. But this approach is not in view of the characteristics and will disclose more information than feature templates if it is cracked.

In view of the shortcomings of the approaches above, we propose a hybrid approach for face template protection. The proposed approach on the basis of the lower dimensional feature extracting combine the theory of chaos and RSA to encrypt the template directly. After the change of dimension and data the encrypted template is obtained.

2. Method

The proposed method is to obtain the safe and reliable face feature template encrypted by the intermediate data of face recognition system, applying $2D^2$LDA and PCA as the feature extraction method. The $2D^2$LDA method can reduce the dimension in two directions so that only very little template data need to be stored. And the PCA is a classic feature extraction method. Because the elements of the original feature matrix $Q_{M\times N}$ obtained by feature extraction algorithms are not are not suitable for encryption, a pretreatment for each element is needed. After saving two decimal places of every element, an integer matrix $A_{M\times N}$ can be obtained as:

$$A_{M\times N} = Q_{M\times N} \times 10^2$$

Then the proposed approach changed the position and value of the elements of matrix $A_{M\times N}$. The proposed protecting framework is shown in Figure 1.

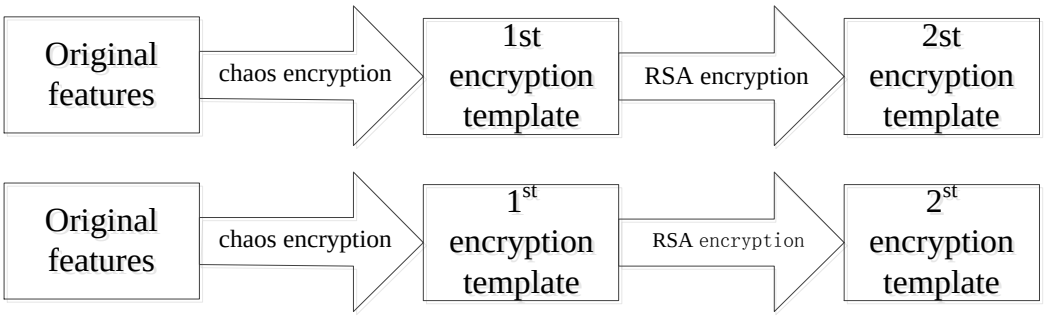

Figure 1. The Proposed Framework for Protecting Face Biometric Template

2.1. 1st Encryption by Chaos

Chaos was given the concept by the American meteorologist Lorenz through the study on the atmospheric circulation in 1963[13]. In recent years, encryption based on chaos theory has been widely used in various fields. In the field of image processing, the

pseudo random chaotic sequence is used to encrypt the images. Therefore, a lot of chaotic sequence generation algorithms with excellent properties are generated. For example, one-dimensional Logistic map, two-dimensional Henon map, three-dimensional Lorenz map and other higher dimensional maps, etc. In the process of applying the chaotic sequence, according to different application environment the chaotic sequence is divided into the real number sequence, the binary sequence and the bit sequence [14-16].

The proposed approach use bit sequence processing to treat the pseudo random sequence $\{x, y\}$ generated by 2D Logistic map to obtain the scrambling matrix and the initial RSA key respectively. The 2D Logistic cat map is as follows:

$$\begin{cases} x_{n+1} = \mu\alpha_1 x_n(1-x_n) + \beta y_n \\ y_{n+1} = \mu\alpha_2 y_n(1-y_n) + \beta x_n \end{cases} \quad (1)$$

Where, $n = 0,1,2\cdots\cdots$, $(x_0, y_0) \in (0,1)$. When $\mu = 4$, $\alpha_1 = 0.9$, $\alpha_2 = 0.9$, $\beta = 0.1$, the system is in a state of chaos. And the process of the chaotic sequence is shown in Figure 2.

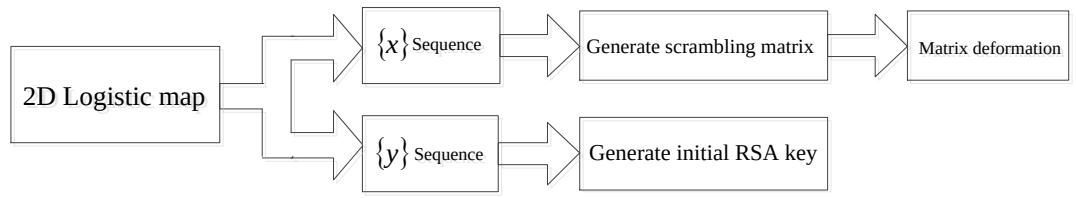

Figure 2. The Process of the Chaotic Sequence

2.1.1. $\{x\}$ **Sequence Process:** Focus on matrix $A_{M\times N}$ and sequence $\{x\}$. Given the cycle times parameter n_x, the extraction location parameter s_x and the extraction number parameter m_x ($m_x = M \times N$). Thus, the scrambling matrix $T_{M\times N}$ can be generated according to the given parameters. And then, use $T_{M\times N}$ to encrypt the matrix $A_{M\times N}$ will obtain an encrypted matrix $B_{M\times N}$.

In the entire encryption algorithm not only the original matrix will be scrambling, the encrypted matrix $B_{M\times N}$ should also be deformed according to the key size of RSA and produce the matrix $C_{M'\times N'}$. The purpose of this deformation is to change the length of the RSA algorithm, and to reduce the size of the final storage template. Next, connect the elements of each row of the matrix $C_{M'\times N'}$ to make it into matrix $D_{M'\times 1}$ and generate help data matrix $R_{M'\times N'}$. The help data matrix $R_{M'\times N'}$ records the number of characters and the symbols corresponding to $C_{M'\times N'}$, which is used to recover the matrix $C_{M'\times N'}$ into $A_{M\times N}$. The matrix transformation process is shown as follows:

$$A_{M\times N}\begin{Bmatrix} a_{11} & a_{12} & \cdots a_{1N} \\ a_{21} & a_{22} & \cdots a_{2N} \\ \vdots & & \vdots \\ a_{M1} & a_{M2} & \cdots a_{MN} \end{Bmatrix} \Rightarrow B_{M\times N}\begin{Bmatrix} b_{11} & b_{12} & \cdots b_{1N} \\ b_{21} & b_{22} & \cdots b_{2N} \\ \vdots & & \vdots \\ b_{M1} & b_{M2} & \cdots b_{MN} \end{Bmatrix} \Rightarrow C_{M'\times N'}\begin{Bmatrix} c_{11} & c_{12} & \cdots c_{1N'} \\ c_{21} & c_{22} & \cdots c_{2N'} \\ \vdots & & \vdots \\ c_{M'1} & c_{M'2} & \cdots c_{M'N'} \end{Bmatrix}$$

$$\Rightarrow D_{M'\times 1}=\begin{Bmatrix} d_{11} \\ d_{21} \\ \vdots \\ d_{M'1} \end{Bmatrix}=\begin{Bmatrix} c_{11}c_{12}c_{13} & \cdots c_{1N'} \\ c_{21}c_{22}c_{23} & \cdots c_{2N'} \\ \vdots & \vdots \\ c_{M'1}c_{M'2}c_{M'3}\cdots c_{M'N'} \end{Bmatrix} \qquad R_{M'\times N'}=\begin{Bmatrix} r_{11} & r_{12} & \cdots r_{1N'} \\ r_{21} & r_{22} & \cdots r_{2N'} \\ \vdots & & \vdots \\ r_{M'1} & r_{M'2} & \cdots r_{M'N'} \end{Bmatrix}$$

(2)

The specific M' and N' values should be selected according to the RSA encryption conditions, and the details will be described in the below.

2.1.2. $\{y\}$ **Sequence Process:** Focus on the key length of (p,q) in the RSA algorithm. Given the cycle times parameters (n_{yp},n_{yq}), the extraction location parameters (s_{yp},s_{yq}) and the extraction number parameters (m_{yp},m_{yq}). Assuming that the key length is (l_p,l_q) and extracting one integer in each iteration according to the given parameters we can produce numerical sequence $\{Z_{ypm},m=1,2,\cdots,m_{yp}\}$ and $\{Z_{yqm},m=1,2,\cdots,m_{yq}\}$ $(m_{yp}=l_p,m_{yq}=l_q)$. Then connecting the elements of each numerical sequence we can obtain (p,q). The (p,q) generation process is shown as follows:

$$\{Z_{ypm}\}=\{Z_{yp1},Z_{yp2},\quad\cdots,Z_{ypm}\}\ \Rightarrow\ \{p\}=\left\{\underbrace{Z_{yp1}Z_{yp2}Z_{yp3}\cdots\quad\cdots Z_{ypm}}_{l_p}\right\}$$

$$\{Z_{yqm}\}=\{Z_{yq1},Z_{yq2},\ \cdots,Z_{yqm}\}\ \Rightarrow\ \{q\}=\left\{\underbrace{Z_{yq1}Z_{yq2}Z_{yq3}\cdots\ \cdots Z_{yqm}}_{l_q}\right\} \tag{3}$$

After getting the initial sequence (p,q), a series of processing is needed to meet the requirements of the RSA algorithm. The sequence process steps are shown as follows:

Step1: guarantee (p) is a prime number according to the laws of the primes;

Step2: judging whether the sequence (p) is a strong prime number according to the strong prime check method;

Step3: if (p) is not a strong prime sequence, add 2 into (p) and return to Step2; If (p) is a strong prime sequence, then sequence (p) can be used as an initial key of RSA algorithm.

After the same operation to the sequence (q) the other keys can be calculated, and then turns into the RSA encryption process.

The $\{y\}$ sequence process will take a lot of time to get (p,q), but this part is not belong to the encryption process that can be done in isolation, so that it will not affect the overall encryption time of the algorithm.

2.2. 2nd Encryption by RSA

RSA encryption algorithm belongs to asymmetric encryption system [17]. It is designed by three mathematicians Rivest, Shamir and Adleman according to the Whitfield and Martin Hellman's theoretical framework in 1977 and named it after the three scientists' initials. RSA algorithm is based on an arithmetic fact that multiplication of two large prime Numbers together is very easy, but factorization for the result of multiplication is extremely difficult. So the product can be used as an encryption key and open.

The key parameters of RSA encryption: p , q , n , $\phi(n)$, e , d . Where n is the modulus, e is the public key, d is the private key. And the parameters are calculated as follows:

$$n = p \times q \tag{4}$$

$$\phi(n) = (p-1) \times (q-1) \tag{5}$$

$$e \times d = 1 \bmod (\phi(n)) \tag{6}$$

The determination of parameters: (1) n is determined by two large primes p and q . So the difference between p and q should larger enough, the greatest common factor of $p-1$ and $q-1$ is smaller; (2) the public key e and $\phi(n)$ are coprime; (3) the private key d should be greater than $n^{0.25}$[18].

Encryption:

$$C = M^e \bmod n \tag{7}$$

Decryption:

$$M = C^d \bmod n \tag{8}$$

In the proposed approach, RSA algorithm is applied to encrypt the element of each row in matrix $D_{M'\times 1}$, and finally getting the security encryption template $E_{M'\times 1}$.

$$D_{M'\times 1} = \begin{Bmatrix} d_{11} \\ d_{21} \\ \vdots \\ d_{M'1} \end{Bmatrix} \Rightarrow E_{M'\times 1} = \begin{Bmatrix} e_{11} \\ e_{21} \\ \vdots \\ e_{M'1} \end{Bmatrix} \tag{9}$$

In the application of RSA algorithm, the text that going to be encrypted must less than the modulus n . So each element of matrix $D_{M'\times 1}$ must smaller than n . In other words, in

the process of dealing with chaotic sequence $\{x\}$ to obtain $D_{M'\times 1}$ must ensure that the sum of bits of each row element in matrix $C_{M'\times N'}$ must smaller than n. The sum of element in each row of help data matrix $R_{M'\times N'}$ is smaller than n.

$$\begin{cases} r_{11} + r_{12} \cdots + r_{1N'} = r_1 < n \\ r_{21} + r_{22} \cdots + r_{2N'} = r_2 < n \\ \vdots \\ r_{M'1} + r_{M'2} \cdots + r_{M'N'} = r_{M'} < n \end{cases} \tag{10}$$

3. Enrollment and Authentication

This paper proposes an encryption algorithm that can be used in face recognition and matching system. This section gives out the detail operation steps and the matching scheme. The flow chart of the algorithm is as follows:

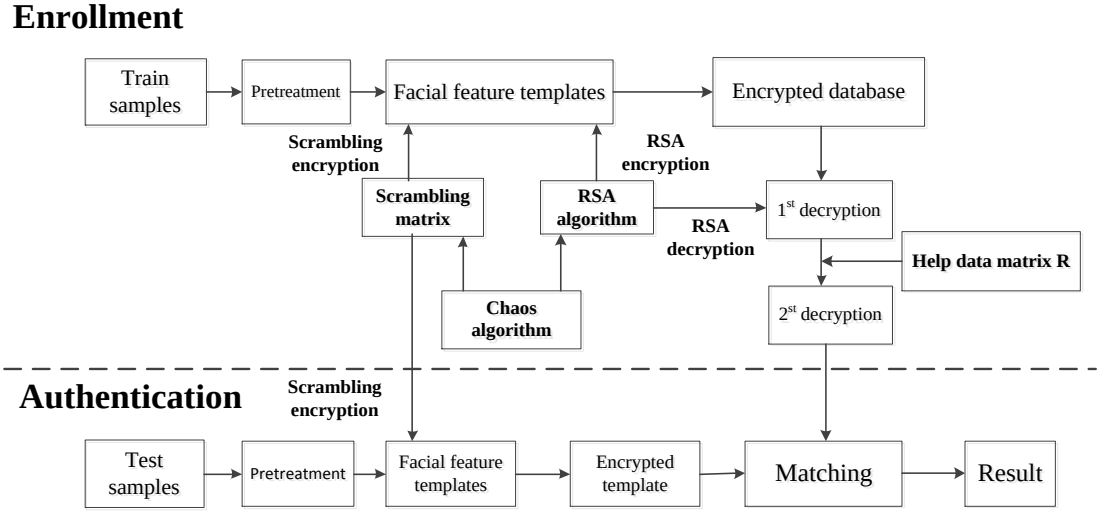

Figure 3. The Flow Chart of the Proposed Algorithm

3.1. Enrollment Steps

Step1: input a $m \times n$ training face from ORL database and get the matrix $A_{M\times N}$ by feature extraction methods and template pretreatment;

Step2: compute the sequence $\{x, y\}$ according to the initial parameters $\{(x_0, y_0), \mu, \alpha_1, \alpha_2, \beta\}$ of chaos;

Step3: get the scrambling matrix $T_{M\times N}$ and the key $\{p, q\}$ of RSA;

Step4: apply $T_{M\times N}$ to scramble the matrix $A_{M\times N}$, and connect its elements of each row to generate matrix $D_{M'\times 1}$ and help data matrix $R_{M'\times N'}$;

Step5: encrypt each row of matrix $D_{M'\times 1}$ with RSA algorithm, finally getting the encrypted template $E_{M'\times 1}$ and the encrypted ORL database.

3.2. Authentication Steps

Step1: extract the features of the authentication face, and obtain the matrix $A'_{M\times N}$ after preprocess;

Step2: release the matrix $T_{M\times N}$ to encrypt $A'_{M\times N}$ to get matrix $B'_{M\times N}$;

Step3: release the RSA private key to decrypt the database

Step4: release help data matrix $R_{M'\times N'}$ to decrypt the database for the second time;

Step5: computing the matching results.

4. Experimental Data and Results

The experimental results here are based on 2D^{2}LDA and PCA systems and the proposed algorithm is used to encrypt the template extracted by the two feature extraction algorithm. This section gives out the specific data in the process, the data contrast between different deformation of the same parameters and different parameters of the same features, and the matching results.

4.1. The Results of 2D^{2}LDA System

4.1.1. Feature Matrix Preprocessing Results: Randomly choose a 92×112 training image and extract its 16×16 facial feature template $Q_{16\times16}$. Keep two decimal places of every element of $Q_{16\times16}$ to get the integer matrix $A_{M\times N}$ without affecting the final matching rate. The data processing procedures are as follows:

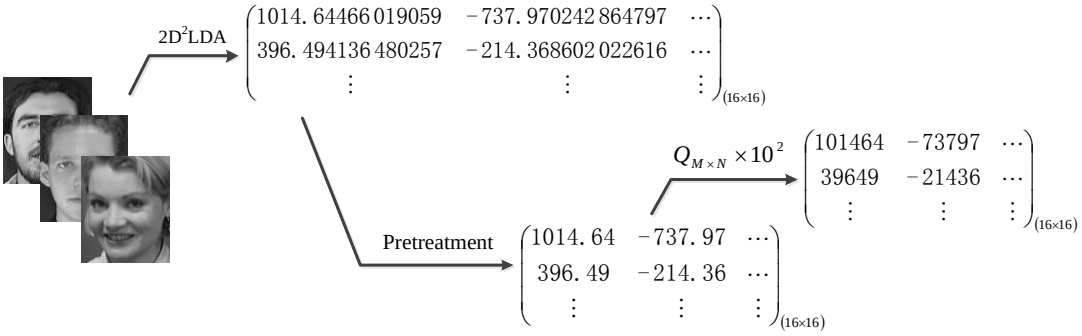

Figure 4. Data Processing Procedures

4.1.2. The Generation of Scrambling Matrix and RSA Parameters: Give out the initial value of chaos as $(x_0 = 0.123, y_0 = 0.124)$. Define the initial parameters of $\{x\}$ is $(n_x = 500, s_x = 11, m_x = 256)$.That means give up the first 500 iterations to guarantee the chaotic characteristics of the system, then extract 256 elements to generate the scrambling matrix $T_{16\times16}$ from the eleventh after the decimal point of each iteration. For $\{y\}$ is $\{(n_{yp} = 500, n_{yq} = 1000),(s_{yp} = 11, s_{yq} = 11),(m_{yp} = 155, m_{yq} = 155)\}$, and the two 512bit sequences (p,q) can be generate. Finally, the other parameters of RSA can be obtained, too.

4.1.3. The Best Method for Deformation: The length of each element of the matrix is different under different deformation conditions, so a good deformation can reduce the

size of the final template effectively. Figure 5 shows the length of each row with different deformations. When the longest element of matrix D is close to the modulus n, the number of rows will no longer be reduced, and the best deformation can be obtained.

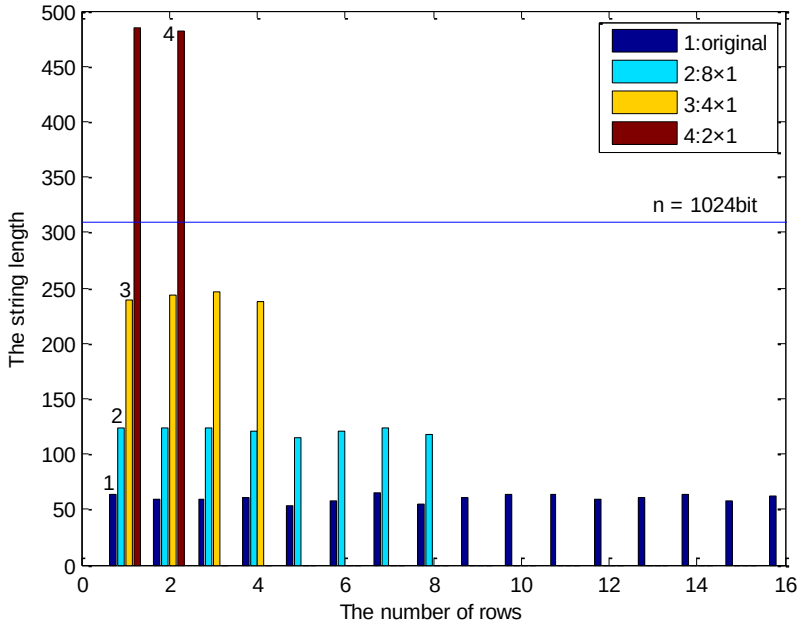

Figure 5. The Comparison of the Length for Each Line with Different Deformation

Table 1 shows the specific data under different deformation. When the maximum length is close and no more than the modulus n, the best deformation changed matrix 16×16 to 4×64 and the final template is 4×1.

Table 1. The Specific Data of the Same Template under Different Deformation

	16×16	8×32	4×64	2×128
After deformation	16×1	8×1	4×1	2×1
Max line	65	124	246	485
Min line	54	115	237	481
After encryption	16×1	8×1	4×1	Over range

4.1.4. The comparison under different scrambling parameters: Now we have already got the matrix $B_{16\times16}$ after scrambling and the best 4×64 deformation method. Because of the deformation only affects the stored template, has nothing to do with the safety of the algorithm. Therefore, in order to makes the experiment data more clearly here we give out the comparison data between different scrambling parameters under the same deformation directly.

Figure 6 shows the length of each row in the condition that only x_0 small changes, only y_0 small changes and different secret key n_x .The result suggests that the change of length have no rules, but close.

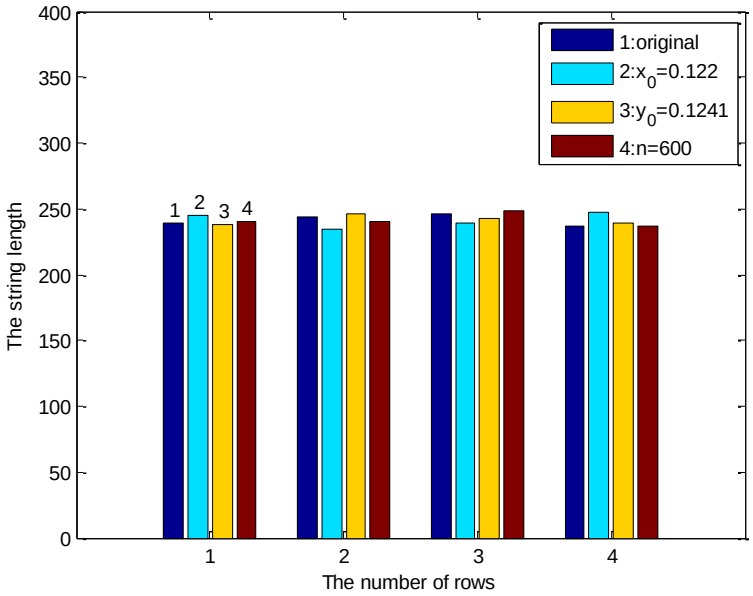

Figure 6. The Comparison of the Length for Each Line with Different Scrambling Parameters

Table 2 shows the specific data under different scrambling parameters. When arbitrary parameters have a slight change, the length has not much volatility, and will not affect the RSA encryption.

Table 2. The Specific Data of the Same Template under Different Scrambling Parameters

	Original	$x_0 = 0.122$	$y_0 = 0.1241$	$n_x = 600$
1st line	239	245	238	240
2st line	244	235	246	240
3st line	246	239	243	249
4st line	237	247	239	237

Under the same deformation, the matrix with different parameters not only has different length, the sequence of each row is also completely different. After add sequence $\{y\}$ and $\{(n_{yp}, n_{yq}),(s_{yp}, s_{yq}),(m_{yp}, m_{yq})\}$, can produce different n, e and d to make the template more secure.

4.1.5. The Comparison of the Recognition Rate: This section shows the recognition rate in the 2D^{2}LDA system which applied the proposed algorithm. The Euclidean distance is

$$d = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{11}$$

It can be seen that the matching results are not related to the position of the matrix elements, we don't need this decrypt process and can save the time. Since the proposed algorithm does not destroy the intermediate data and can be decrypt completely, so the recognition rate is consistent with the original system.

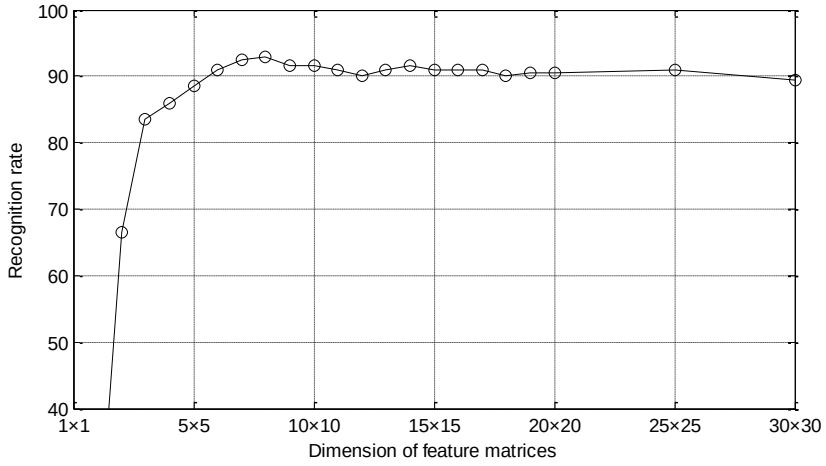

Figure 7. The Recognition Rate of Original System

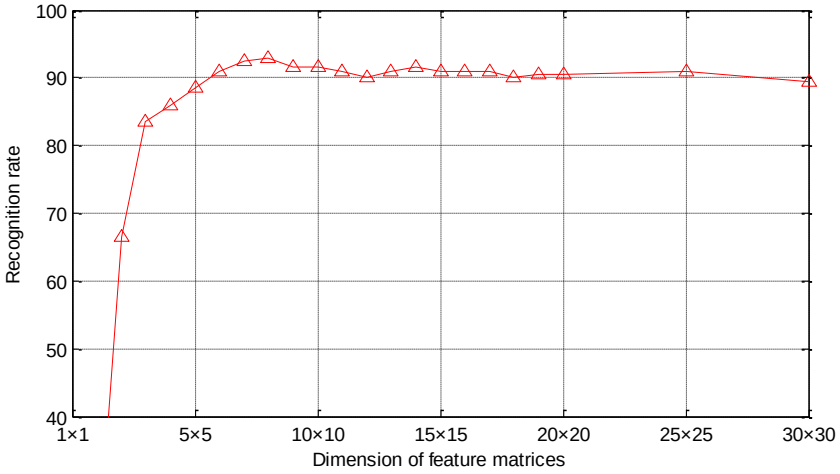

Figure 8. The Recognition Rate of Proposed Method

4.2. The Results of PCA System

4.2.1. Feature Matrix Preprocessing Results: According to PCA, reshape an 92×112 image into a 1×10304 row vector, and then reduce the dimension of the original image to $1 \times 71$by select the eigenvalues and the eigenvectors with 90% of the total variance. And in order to deformation add elements "0" to become1×72.The same with 2D^{2}LDA keep two decimal places of every element to get the integer matrix $A_{1\times 72}$ without affecting the final matching rate.

4.2.2. The Generation of Scrambling Matrix and RSA Parameters: Give out the initial value of chaos as $(x_0 = 0.123, y_0 = 0.124)$. Define the initial parameters of $\{x\}$ is $(n_x = 500, s_x = 11, m_x = 72)$. Give up the first 500 iterations to guarantee the chaotic characteristics of the system, then extract 72 elements to generate the scrambling matrix

$T_{1\times72}$ from the eleventh after the decimal point of each iteration. The key of RSA is the one that generated last time.

4.2.3. The Best Method for Deformation: Because of PCA extracts a one-dimensional matrix, so the initial matrix is 1×72. Figure 9 shows the number of each row with different deformations. Table 3 shows the specific data under different deformation.

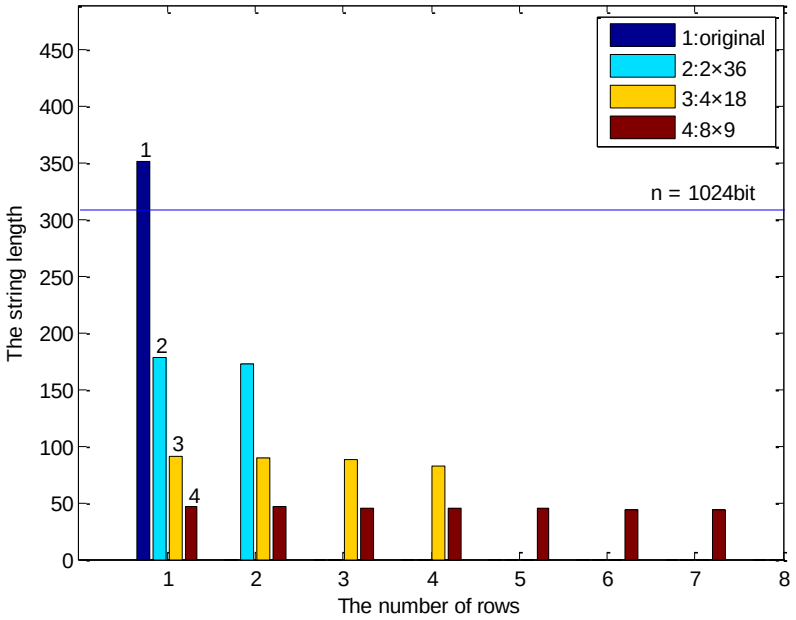

Figure 9. The Comparison of the Length for Each Line with Different Deformation

Table 3. The Specific Data of the Same Template under Different Scrambling Parameters

	1×72	2×36	4×18	8×9
After deformation	1×1	2×1	4×1	8×1
Max line	352	179	91	46
Min line	352	173	83	38
After encryption	Over range	2×1	4×1	8×1

The experimental results show that the best deformation of PCA is 2×36.

4.2.4. The Comparison under Different Scrambling Parameters: Figure 10 shows the number of each row with different scrambling parameters, and Table 4 shows the specific data.

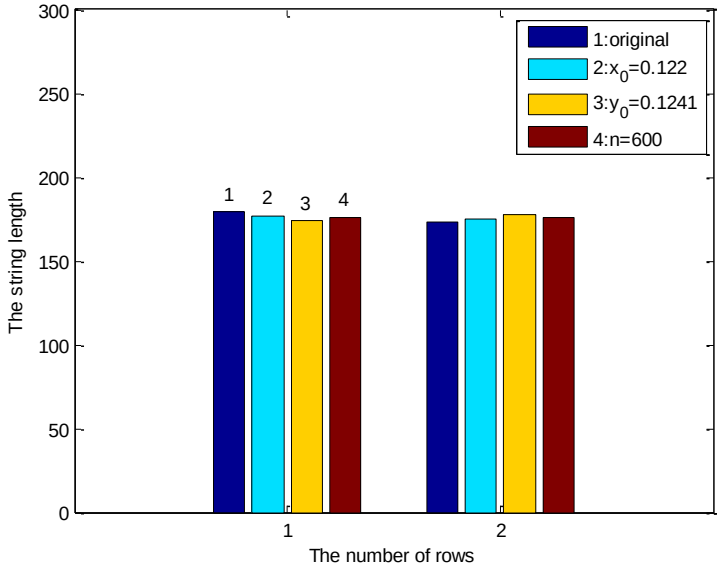

Figure 10. The Comparison of the Length for Each Line with Different Scrambling Parameters

Table 4. The Specific Data of the Same Template under Different Scrambling Parameters

	Original	$x_0 = 0.122$	$y_0 = 0.1241$	$n_x = 600$
1st line	179	177	174	176
2st line	173	175	178	176

4.2.5. The Comparison of the Recognition Rate: This section shows the recognition rate in the PCA system which applied the proposed algorithm. The matching scheme is the same with $2D^2LDA$.

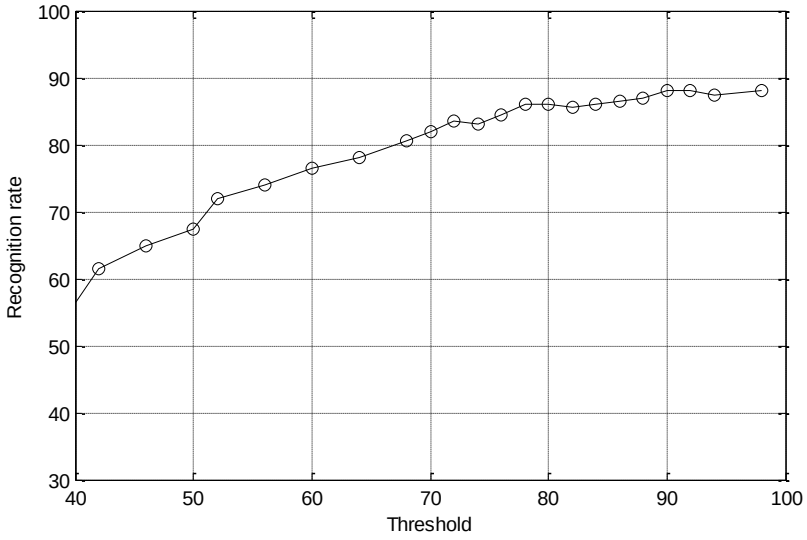

Figure 11. The Recognition Rate of Original System

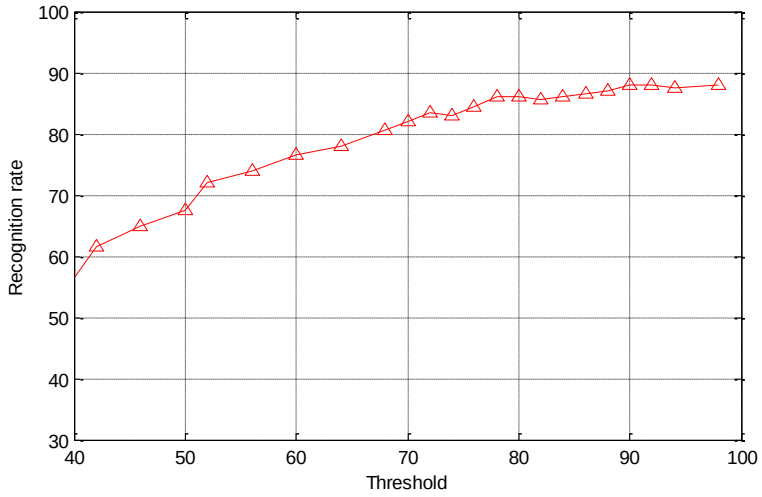

Figure 12. The Recognition Rate of Proposed Method

5. Security Analysis

The hybrid encryption algorithm proposed in this paper combined with scrambling process with RSA algorithm, and finally obtain the new template that completely different from the original. Here gives the security analysis of the algorithm.

5.1. Larger Key Space

The key space of proposed hybrid algorithm is significantly bigger than the traditional chaos algorithm. The ultimate goal of parameters (n_x, s_x, m_x) is to scramble matrix $A_{M\times N}$. Although the matrix dimension extracted by feature extraction algorithm is very small, it still has 256! kinds of schemes. After scrambling, no matter which parameter is changed the key of RSA is far from the last one and lead to different results.

So this approach is in accordance with the requirements of encryption. Meanwhile it is also contains erotic property, randomness and sensitivity to initial value of the chaos algorithm.

5.2. Analysis of 1204bit RSA Algorithm

The formula of RSA algorithm is not complicated. But in the course of several decades has been tested by practice RSA has become a world recognized, secure encryption method. Generally speaking, there are two categories of attacks to crack RSA algorithm. One is due to the improper selection and application of the key, include the small decryption key attack and the common modulus attack. The other is due to the improvement of technology reduced the cost of cracking, makes it easier to decompose modulus n. The first type of attack requires reasonable selection for each key. But the second one has close contact with the hardware development.

In 1999, researchers took 5 months to break a 512bit key. In 2009, 768bit secret key is attacked by factorization. The time required for the decomposition of 768bit is thousands of times than 512bit, and the time to decompose 1024bit is longer than 768bit more than one thousand times. So many experts predict that 1024bit key is still safe.

5.3. Data Leakage Analysis

A fragile system is the stability will be affected when only a few parameters were leaked, and that's not what people expected. So we need a system that can still stable in the worst case. The given parameters are all the key needed by 2D-Logistic system, but after calculation it is divided into the scrambling key and the prime generation key. If the encrypted template is safe when the parameters were leaked, then the proposed algorithm is reliable.

When the scrambling key leaked but RSA parameters are safe, attackers will face the 1024bit RSA cipher text matrix E . Now the RSA algorithm can well protect the safety of the template. When the RSA parameters leaked but scrambling key is safe, the plaintext matrix D will be obtained. The each row of matrix is a series of numerical sequence will not reflect the original template. In the worst case that all of the secret keys were leaked in the system, we can only cancel the original security template. No matter which the secret parameter is changed, the new template will be totally different from the last one. And according to the characteristics of RSA algorithm, the original parameters will not able to decrypt the new template correctly.

6. Conclusion

To protect face feature template, a hybrid algorithm of chaos and RSA encryption has been proposed. After truncated the original template added scrambling, deformation and consolidation. At last, the value was changed by RSA encryption. The experimental results show that the encrypted template is quite different from the original in shape and form. The algorithm has higher safety performance and can be decrypted expediently and intact preserve the recognition effect of the original system.

Acknowledgements

This work was supported by the project for young creative talents of colleges and universities in Heilongjiang Province (UNPYSCT-2015039). The authors also would like to express their deep appreciation to all anonymous reviewers for their kind comments.

References

[1] O. S. Adeoye, J. “A survey of emerging biometric technologies”, International Journal of Computer Applications, vol. 10, **(2010)**.
[2] K. B. Raja, J., “Fingerprint recognition using minutia score matching. International Journal of Engineering Science & Technology”, 1001.4186 **(2010)**.
[3] S. M. Mohsen, S. M. Zamshed Farhan and M. M. A. Hashem, J., “Automatic Fingerprint Recognition Using Minutiae Matching Technique for the Large Fingerprint Database”, Computer Science, **(2013)**.
[4] F. S. Samaria and A. C. Harter, “Parameterisation of a stochastic model for human face identification”, Proceedings of the Second IEEE Workshop on Applications of Computer Vision, Sarasota, FL, **(1994)** December 5-7.
[5] G. Shakhnarovich and B. Moghaddam, Editor, “Face recognition in subspaces”, Handbook of Face Recognition, Springer London, **(2011)**.
[6] Y. Deng, Z. Guo and Y. Chen, “Fusing Local Patterns of Gabor and Non-subsampled Contourlet Transform for Face Recognition”, 2nd IAPR Asian Conference on Pattern Recognition (ACPR), Naha, Japan, **(2013)** November 5-8.
[7] A. K. Jain, K. Nandakumar and A. Nagar, J. “Biometric template security”, EURASIP Journal on Advances in Signal Processing, vol. 113, **(2008)**.
[8] Q. Wang, W. Huang, X. Niu and X. Jiang, “A Template Protection Scheme For Statistic Feature-based 2D Face Recognition”, Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, **(2008)** August 15-17.
[9] A. Juels and M. Wattenberg, “A fuzzy commitment scheme”, Proceedings of the 6th ACM conference on Computer and communications security, Kent Ridge Digital Labs, Singapore, **(1999)** November 2-4.
[10] Y. C. Feng, P. C. Yuen and A. K. Jain, J. “A hybrid approach for generating secure and discriminating face template”, IEEE Transactions on Information Forensics and Security, vol. 5 **(2010)**.

[11] Y. C. Wu, Y. C. Fang and Y. Tan, J. "Face-hashing Algorithm Based on Fuzzy Cyclic Random Mapping", Computer Science, vol. 39, **(2012)**.
[12] D. James and M. Philip, J. "A Novel Face Template Protection Scheme based on Chaos and Visual Cryptography", International Journal of Applied Information Systems, vol. 2, **(2012)**.
[13] E. N. Lorenz, J. "Deterministic nonperiodic flow", Journal of the atmospheric sciences, vol. 20, **(1963)**.
[14] Y. Wang, J. "Image Encryption Based on Chaotic Sequences", Computer Engineering and Applications, vol. 38, **(2002)**.
[15] L. H. He, J. P. Zhang and Q. Wang, J. "Digital Image Watermark Algorithm Based on Wavelet Transform and Compound Chaotic System", Journal of Harbin University of Science and Technology, vol. 15, **(2010)**.
[16] M. J. Yang, X. J. Fan and S. C. Yu, J. "Encryption Algorithm Based on 3D Chaotic Mapping in HSV Space", Journal of Harbin University of Science and Technology, vol. 20, **(2015)**.
[17] R. L. Rivest, A. Shamir and L. Adleman, J. "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, **(1978)**.
[18] B. Dan, G. Durfee and Y. Frankel, "An attack on RSA given a small fraction of the private key bits", Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology, Beijing, China, **(1998)** October 18-22.