Template Protection Based on Chaotic Map for Face Recognition

Jinjin Dong[1], Xiao Meng[1], Meng Chen[1], Zhifang Wang[1](✉),
and Linlin Tang[2]

[1] Department of Electronic Engineering,
Heilongjiang University, Harbin, Heilongjiang, China
xiaofang_hq@126.com
[2] Harbin Institute of Technology Shenzhen Graduate School,
Xili, Shenzhen, China

Abstract. With the widespread deployment of biometric recognition, personal data security and privacy are attracted more and more attentions. A crucial privacy issue is how to ensure the security of user template. This paper proposes a novel template protection algorithm for face recognition based on chaotic map. Each face template is corresponding to different chaotic sequence produced by system master key and user identification number. The order of chaotic sequence controls the substitution index of face template. Experiment results on facial FERET database show that our algorithm can significantly improve the recognition performance and ensure the security of face template.

Keywords: Template protection · Face recognition · Logistic map · Substitution index

1 Introduction

Biometric refers to identify or verify a person according to their physiological or behavioral characteristics such as fingerprint and handwriting. It is an automated process of identification and authentication, in which specific biometric traits of an individual are extracted during enrollment and stored as biometric templates. However, such authentication technology needs large-scale capture and storage of biometric data which leads to serious concern about leaking of privacy and identity theft. Unlike the traditional identification technology such as password or credit card, biometric characteristics are inherent to a person. Once the template is compromised, it is compromised forever because it cannot be revoked, reissued or even destroyed. Furthermore, since the same template might be used for various application and location, it would be possible to perform cross matching between them. In this way, the privacy of the user cannot be guaranteed.

Many template protection algorithms have been proposed. Jain divided these algorithms into two kinds: feature transformation and biometric encryption [1]. The former is a popular scheme in which the same transformation function respectively applies to register biometric characteristics and testing biometric characteristics in enrollment procedure and testing procedure. Then the transformed testing

B. Zou et al. (Eds.): ICPCSEE 2017, Part I, CCIS 727, pp. 242–250, 2017.
DOI: 10.1007/978-981-10-6385-5_21

characteristics directly compares with the transformed template generated by register characteristics. The latter is firstly proposed to use biometric feature to encrypt key. It is deferent from feature transformation is that public information related to the biometric feature is stored in the database. The former security depends on the key safety and noninvertible transforms. And the latter depends on the safety of help data. This paper proposes a face template protection method based on chaotic map which belongs to the former.

Due to the high sensitivity of chaotic systems to parameters and initial conditions as well as the availability of many circuit realizations, chaos based algorithms are developed and studied as the core of encryption algorithms [2]. Chaotic image encryption refers to use discrete chaotic sequence to encrypt the image, and its essence is to play the characteristics of chaos to conceal the original face image and avoid the valuable information being achieved by other people even they get encrypted information [3, 4].

In this paper, an eigenvalues permutation algorithm for face template protection based on chaotic map is proposed. The original face template is extracted using principal component analysis (PCA) algorithm and disturbed based on chaotic logistic map. The rest of the paper is organized as follows: Sect. 2 introduces the existing biometric protection methods. Section 3 gives the proposed algorithm. Section 4 is devoted to the experiments and security analysis. At last, Sect. 5 concludes this paper.

2 Related Works

2.1 Biometric Protection Method

In recent years, there are increasing applications of biometric identification technology in the identity authentication, but also gradually expose its inherent weaknesses in some aspects of security and privacy, so higher requirements of the security of biometric template in the practical applications is raised. The template protection scheme should have properties like diversity, revocability, security and performance. The template protection schemes are broadly classified into two main types as function transformation approach and biometric cryptosystem based approach. Function transformation approach is further categorized as salting and non-invertible transformation method. Biometric cryptosystem based approach is further categorized as key binding and key generation methods.

A large number of famous biometric cryptosystems have been proposed such as fuzzy vault scheme [5–8], fuzzy commitment scheme [9], and fuzzy extractor [10]. Fuzzy vault is used to encrypt the biometric template which is described in the form of point sets, such as fingerprint minutiae sets. The fuzzy vault scheme proposed by Juels and Sudan [5–7] has become one of the most popular key-binding approaches as it provides effective and provable security for biometric template protection [11]. Since the fuzzy vault scheme is proposed, many biometric characteristics have been used to construct biometric cryptosystems based on fuzzy vault scheme, such as fingerprints, ear, and face.

Fuzzy commitment and fuzzy extractor are among the two most popular template protection schemes. Fuzzy commitment binds a binary key to a binary biometric representation and the key can only be recovered if a similar binary biometric re-presentation is presented. Fuzzy extractor directly transforms a binary biometric input into a stable binary string that can be used as encryption keys in cryptographic applications. Both these schemes take an ordered multi-biometric representation as input in our context. When modalities that are represented by un-ordered features are fused with modalities that are represented by ordered features, an unordered-to-ordered feature transformation is required.

3 Proposed Algorithm

A face recognition system firstly collects several face images of each legitimate user and extracts face features stored in the database corresponding with this user's ID number. One of the popular approaches for face recognition is eigenface method (Principal Component Analysis, PCA) [12]. The key idea is to find the best set of projection directions to span the feature space that will maximize the total scatter. Our proposed algorithm adopts PCA to produce face features for each user. So each user's face feature is a vector. Then we use image encryption for reference to displace the order of face feature vector by utilizing chaotic map. This section describes the generalized logistic map and the detail steps of our algorithm.

3.1 Logistic Map

The logistic map is an one-dimensional map and it is very simple and can produce fundamental results on non-linear dynamics, and it attracts many attention in image encryption lately. A simple chaotic logistic map is defined by Eq. (1):

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

Where n is a non-negative integer, x_0 is the initial value of the logistic map, $x_0 \in [0, 1]$, μ is a control parameter. For a fixed value μ, we can get a certain sequence x_n by iteration with an initial value x_0.

Figure 1 shows the bifurcation diagram of the logistic map while μ belongs to (3, 4]. From the bifurcation diagram, we can see that the sequences generated by logistic map are chaotic sequences when $3.57 < \mu \leq 4$.

Figure 2 shows the Lyapunov exponent curve of logistic and generalized logistic maps. Generally, the Lyapunov exponent is usually taken as an indication that the system is chaotic. If the value of Lyapunov exponent is positive number, the system is chaotic. It is noted that the logistic map has some drawbacks such as non-uniform behaviour and blank windows in the chaotic region as can be seen in Fig. 2(a), there are some areas where the Lyapunov exponent is either zero or negative.

To overcome the issue of the logistic map, we introduce a generalized logistic map [13] defined by Eq. (2)

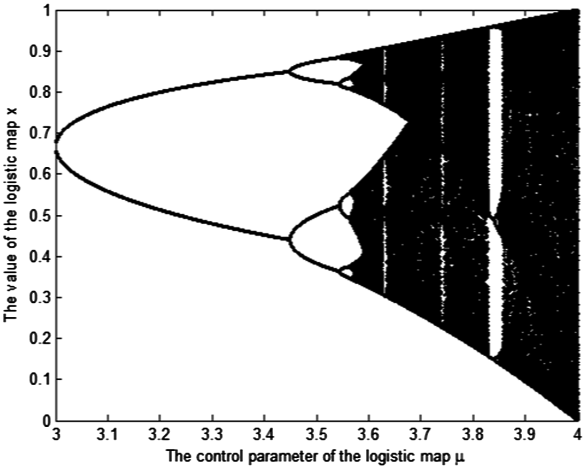


Fig. 1. Bifurcation diagram of the logistic map

$$x_{n+1} = \frac{4\mu^2 x_n(1-x_n)}{1+4(\mu^2-1)x_n(1-x_n)} \tag{2}$$

Where n is a non-negative integer, $-4 < \mu \leq 4$. The logistic map is in the chaotic region when $-4 < \mu \leq -2$ or $2 < \mu \leq 4$. Figure 2(b) shows the Lyapunov exponent of the generalized logistic map. We can see that there is no non-chaotic area in the chaotic region, and the uniform behavior of the generalized map is further proved.

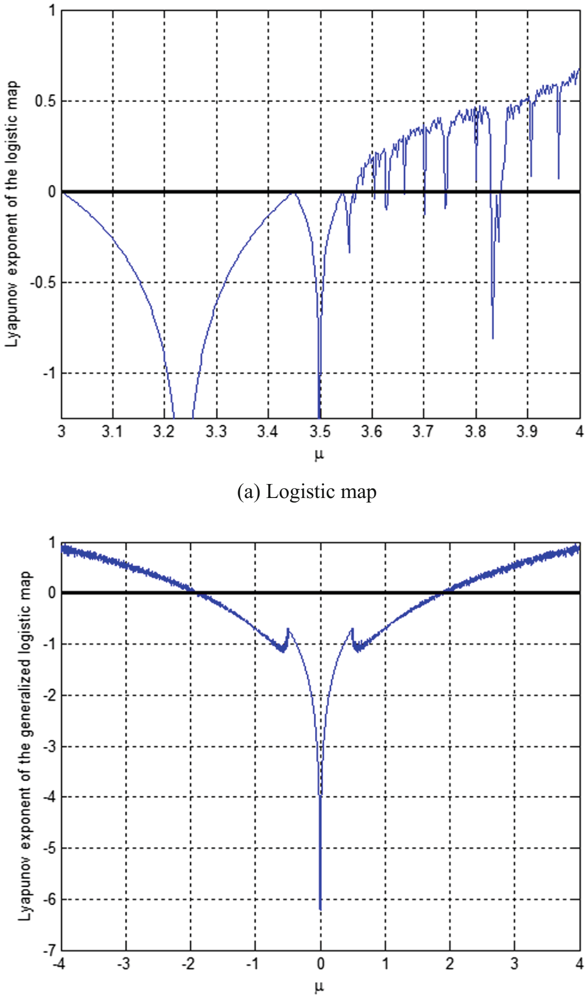
The logistic map has been applied to image encryption since it satisfies the ergodicity, pseudorandom property and extreme sensitive to initial conditions and system parameters.

3.2 Our Algorithm

In this section, we presented our template protection algorithm for face recognition using a position permutation approach for face feature with the chaotic logistic sequences. Each user has its own specific ID, so we use the user ID and the master key of the system to determine the initial conditions of logistic map by hash function. The order of chaotic sequence controls the substitution index of face template. Figure 3 shows the generation process of the face template.

Figure 4 shows an example of the detailed generation flow of the substitution index. For example, the initial value of the logistic map is 0.9, the control parameter of the logistic map is 4, and we choose 10 numbers from the logistic sequence as an example to show the process of the permutation. The method is described in steps as follows:

(1) Encode the master key and user ID to a vector satisfied the input request of hash function, the output of hash function is taken as the initial value of logistic map. Then select an appropriate control parameter through Fig. 2(b), the chaotic



(a) Logistic map

(b) Generalized logistic map

Fig. 2. Lyapunov exponent curves of logistic and generalized logistic maps

logistic sequence is produced. Because different user has different ID, the initial conditions of the chaos are not the same, so the chaotic sequences are different.

(2) Let $V = \{v_1, v_2, \ldots, v_n\}$ be a face feature of the user where n is the dimensionality of eigenvectors, the dimension of chaotic sequence is often great than n. We select the former n dimension of the logistic sequence gained by step (1) as the final used chaotic sequence $L = \{l_1, l_2, \ldots, l_n\}$.

(3) Sort $L = \{l_1, l_2, \ldots, l_n\}$ in ascending order of size and obtain the new sequence $L' = \left\{l'_1, l'_2, \ldots, l'_n\right\}$. Meanwhile, the substitution index $S = \{s_1, s_2, \ldots, s_n\}$ is produced where s_i is the position in L of l'_i. In Fig. 4, 0.9 is the first dimension in L, the corresponding index is seven.

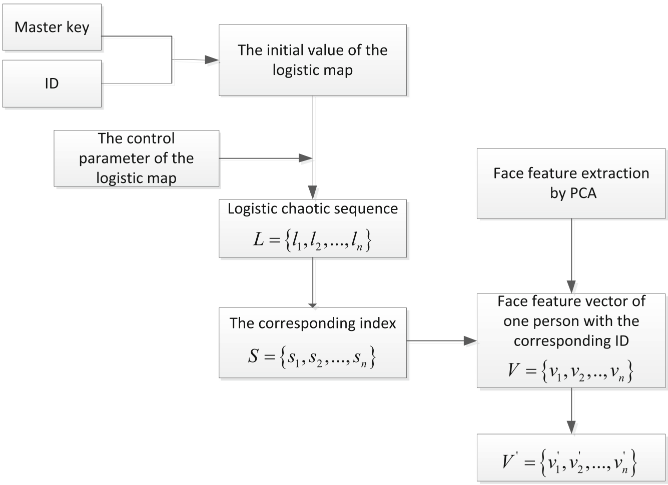
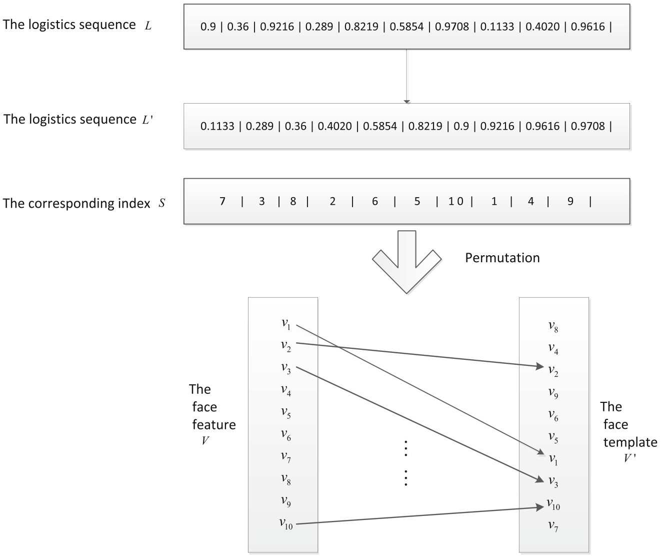

Master key
ID
The initial value of the logistic map
The control parameter of the logistic map
Logistic chaotic sequence
$L = \{l_1, l_2, ..., l_n\}$
Face feature extraction by PCA
The corresponding index
$S = \{s_1, s_2, ..., s_n\}$
Face feature vector of one person with the corresponding ID
$V = \{v_1, v_2, .., v_n\}$
$V' = \{v_1', v_2', ..., v_n'\}$

Fig. 3. The generation process of the face template


The logistics sequence L
The logistics sequence L'
The corresponding index S
Permutation
The face feature V
The face template V'
v_1 v_2 v_3 v_4 v_5 v_6 v_7 v_8 v_9 v_{10}
v_8 v_4 v_2 v_9 v_6 v_5 v_1 v_3 v_{10} v_7

0.9 | 0.36 | 0.9216 | 0.289 | 0.8219 | 0.5854 | 0.9708 | 0.1133 | 0.4020 | 0.9616 |

0.1133 | 0.289 | 0.36 | 0.4020 | 0.5854 | 0.8219 | 0.9 | 0.9216 | 0.9616 | 0.9708 |

7 | 3 | 8 | 2 | 6 | 5 | 10 | 1 | 4 | 9 |

Fig. 4. An example of the detailed generation flow of the substitution index

(4) $V = \{v_1, v_2, .., v_n\}$ is replaced with $V' = \left\{v_1', v_2', \ldots, v_n'\right\}$ by the same rule of permutation, because the elements of the sequence $V = \{v_1, v_2, .., v_n\}$ and the sequence $L = \{l_1, l_2, \ldots, l_n\}$ are corresponding one by one. $V^{'} = \left\{v_1^{'}, v_2^{'}, \ldots, v_n^{'}\right\}$ is the face template.

(5) All the face features of every user are carried out the above four steps to get a new face template.

(6) In testing, a face image of the user is collected. The mapping matrix attained by PCA in registration process is used to extract the testing feature from the face image. Then the logistic sequence is produced by this user ID and the master key to displace the testing feature. Finally, matching the template stored in the system database according to user ID.

4 Experimental Results and Analysis

4.1 Experiment Data and Performance Parameters

In order to test the proposed algorithm, we conduct experiments on the FERET database, and compare the experimental results with the eigenface method. The FERET database is created by the United States Department of Defense, it is the most authoritative face database at present and it contains 200 individuals and 7 images for each person with different postures, facial expression, and illumination condition. Three samples of each person are used as training set, others are used for test.

The original template is the facial feature vector extracted using PCA algorithm. In the FERET database there are 200 persons, so each person has its own user ID, which means each person has its own corresponding logistic map since the initial value of the logistic map is determined by the user ID and the master key. Here we choose 200 logistic map, the initial conditions of the logistic map is determined by the user ID and the master key with an appropriate transformed function, the control parameter of the logistic map is fixed, we set $\mu = 4$ and at this point the logistic map is entirely in the state of chaos, and it can increase the randomness. And then the new template is generated according to our scheme proposed in this paper.

In our algorithm, we use False match rate (FMR) and False non-match rate (FNMR) to evaluate the performance of the algorithm. FMR and FNMR are the major two parameters of recognition algorithm performance evaluation. In addition, the equal error rate (EER) can measure the overall performance of an algorithm. It unifies FMR and FNMR at the same time. FMR increases with the increase of the threshold and FNMR decreases with the increase of the threshold. EER refers to the value of the intersection of FNMR and FMR in the same coordinate. For a high-performance algorithm, there is a smaller value of EER. The DET curve is similar to EER, x axis and y axis represent FMR and FNMR respectively. The Lower DET curve means the higher performance.

4.2 Experimental Results and Security Analysis

Figure 5 shows the DET curve with eigenface and the proposed algorithm. Experimental results show that the ERR of eigenface and the proposed algorithm are 14.2% and 8% respectively. From the graph, we can see more clearly and directly that the performance of our proposed algorithm using the logistic map is better than the original PCA algorithm.

In system, we store four data: the mapping matrix of PCA, user ID, the control parameter of logistic map and the face templates. The security of our algorithm depends

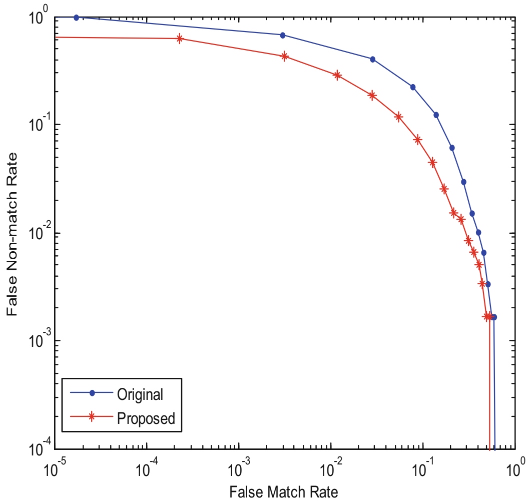


Fig. 5. The comparison of DET curve

on the logistic map. If the attacker doesn't know the logistic sequence, he can't recover the original face feature. The control parameter can't produce the logistic map without the initial condition. The master key and user ID conduct the initial condition by hash function. The irreversibility of hash ensures the security of the master key. The master key is the superlative key of the system, and it is used to protect the primary key and the encryption key. Generally speaking, it is very difficult to attack the master key directly, because the master key is usually stored in a dedicated cryptographic device, it is secure not only physically, but also logically. The master key is only mastered by a few security managers, these security managers are not directly contact to the user's key and plaintext data. And it is not possible for the user to obtain the master key that the security manager has, which is helpful to ensure the security of the key.

In our scheme, we can generate a new feature template by changing the control parameters of chaotic map or changing the master key. In this way, if the original template is destroyed or stolen, you can change the relevant parameters to generate a new template to replace the original template.

5 Conclusion

In this paper, we presented a template protection algorithm for face recognition using chaotic map. We use the properties of the logistic map, such as the ergodicity, pseudorandom property and extreme sensitive to initial conditions and system parameters to generate a chaotic sequence, and the original face feature can be displaced by the chaotic sequences. Since the representation of disturbed template features is the same as before, we can use the same matching scheme to measure the performance of the face recognition system. Experiment results show that our algorithm significantly improve the recognition performance and ensure the security of face template.

Acknowledgments. This work is supported by the National Science Foundation of China (nos. 61201399, 61501176, 61601174), and Startup Fund for Doctor of Heilongjiang University.

References

1. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP J. Adv. Sig. Process. **2008**, 1–17 (2008)
2. Nandakumar, K., Pankanti, S., Jain, A.K.: Fingerprint-based fuzzy vault implementation and performance. IEEE Trans. Inf. Forensics Secur. **2**(4), 744–757 (2007)
3. Kocarev, L., Lian, S.: Chaos-Based Cryptography Theory. Algorithms and Applications. Springer, Heidelberg (2011). doi:10.1007/978-3-642-20542-2
4. Abd-El-Hafiz, S.K., Radwan, A.G., AbdElHaleem, S.H., Barakat, M.L.: A fractal-based image encryption system. IET Image Process **8**(12), 742–752 (2014)
5. Juels, A., Sudan, M.: A fuzzy vault scheme. In: IEEE International Symposium on Information Theory, Switzerland, pp. 408–413 (2002)
6. Uludag, U., Pankanti, S., Jain, A.K.: Fuzzy vault for fingerprints. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 310–319. Springer, Heidelberg (2005). doi:10.1007/11527923_32
7. Barakat, M.L., Mansingka, A.S., Radwan, A.G., Salama, K.N.: Hardware stream cipher with controllable chaos generator for colour image encryption. IET Image Process **8**(1), 33–43 (2014)
8. You, L., Wang, Y., Chen, Y., Deng, Q., Zhang, H.: A novel key sharing fuzzy vault scheme. KSII Trans. Internet Inf. Syst. **10**, 453–460 (2012)
9. Lafkin, M., Mikram, M., Ghouzali, S.: Biometric cryptosystems based fuzzy commitment scheme: a security evaluation. Int. Arab J. Inf. Technol. **13**(4), 443–449 (2016)
10. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM J. Comput. **38**(1), 97–139 (2008)
11. Nagar, A., Nandakumar, K., Jain, A.K.: Multibiometric cryptosystems based on feature level fusion. IEEE Trans. Inf. Forensics Secur. **7**(1), 255–268 (2012)
12. Turk, M., Pentland, A.: Face recognition using eigenfaces. In: IEEE Transaction on Pattern Analysis and Machine Intelligence, pp. 586–591 (1991)
13. Song, X., Wang, S., El-Latif, A.A.A., Niu, X.: Quantum image encryption based on restricted geometric and color transformations. Quantum Inf. Process. **13**(8), 1765–1787 (2014)