Fourth International Conference on Natural Computation

A Novel Cryptosystem based on Iris Key Generation

Xiangqian Wu[1], Ning Qi[1], Kuanquan Wang[1], David Zhang[2]
[1]*School of Computer Science and Technology,*
Harbin Institute of Technology (HIT), Harbin 150001, China
{xqwu, wangkq }@hit.edu.cn
[2]*Biometric Research Centre, Department of Computing,*
Hong Kong Polytechnic University, Kowloon, Hong Kong
csdzhang@comp.polyu.edu.hk

Abstract

Biometric cryptography is a technique using biometric features to encrypt data, which can improve the security of the encrypted data and overcome the shortcomings of the traditional cryptography. This paper proposes a novel biometric cryptosystem based on the most accurate biometric feature -- iris. In encryption phase, a quantified 256-dimension textural feature vector is firstly extracted from the preprocessed iris image using a set of 2-D Gabor filters. At the same time, an error-correct-code (ECC) is generated using Reed-Solomon algorithm. Then the feature vector is translated to a cipher key using Hash function. Some general encryption algorithms use this cipher key to encrypt the secret information. In decryption phase, a feature vector extracted from the input iris is firstly corrected using the ECC. Then it is translated to the cipher key using the same Hash function. Finally, the corresponding general decryption algorithms use the key to decrypt the information. Experimental results demonstrate the feasibility of the proposed system.

1. Introduction

Information security is becoming increasingly important in nowadays and cryptography is one of the most effective ways to enhance the information security. In the traditional cryptographic algorithms, such as AES, DES and RSA etc., information is encrypted using cipher key. The simple keys are easy to be memorized while they are also easy to be cracked. And the complex keys are difficult to be cracked while they are also difficult to be remembered and have to be stored in somewhere, which can be stolen or lost. Biometric cryptography, which uses biometric features to encrypt the information, can overcome this problem. Currently, some biometric cryptographic algorithms have been developed based on fingerprints [1-4], iris [5-7], face [8], voice [9], signature [10] and palmprints [11] etc.

Among the common biometric features, iris is the most accurate feature and can be effectively used in biometric cryptography. Davida [5, 6] proposed an iris cryptographic method based on the error-correcting and hashing techniques. This method supposed that the errors of the iris templates used for encryption and decryption were no more than 10%. Actually, these errors should be up to 30%. And the stored error-correcting code may leak biometric information. Hao [7] regarded the difference between the decrypting and encrypting iris codes as noises and used Hadamard code and Reed-Solomon code to correct these noises. The limitation of their system is that the security is somewhat low (the cracking ratio is 2^{-44}). To improve the security, this paper proposes a novel cryptosystem based on iris key generation. The Reed-Solomon error-correcting algorithm and Hash function are employed to translate the iris textural feature vector to a cipher key for encryption and decryption.

The rest of this paper is organized as follows. Section 2 introduces the framework of our cryptosystem. Section 3 presents the process of iris feature vector extraction. Section 4 discusses the encrypting and decrypting processes. Section 5 contains some experimental results and analysis. And Section 6 provides some conclusions.

2. Framework of the Proposed System

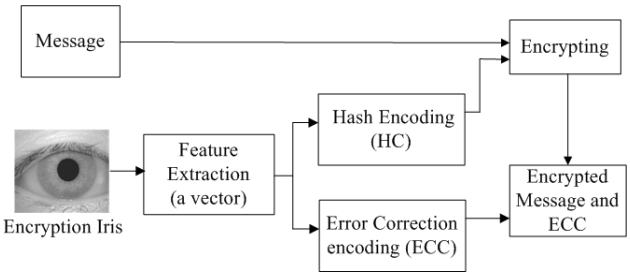
As we know, for a traditional symmetrical cryptographic system, the decrypting key should be exactly identical with the encrypting key. However, the features extracted from the different images of the same iris always have some difference, which may be caused by CCD camera pixel noise, iris distortion, eyelashes and eyelids occlusion etc. Therefore, the iris features cannot be directly used as a cipher key. To solve this problem, this paper uses some error-correcting algorithm to eliminate the difference.

Fig. 1 shows the frameworks of the iris cryptosystem. During the encryption phase, a quantified textural feature vector (FV) is firstly extracted from the encryption iris. At the same time, an error-correct-code (ECC) is generated using Reed-Solomon algorithm. Then the feature vector is translated to a cipher key using a Hash function. Some

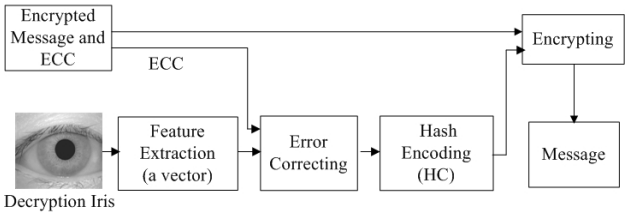
978-0-7695-3304-9/08 $25.00 © 2008 IEEE
DOI 10.1109/ICNC.2008.808

general encryption algorithms use the key to encrypt the secret message.

When decrypting, an iris feature vector extracted from the input iris is firstly corrected using the ECC. Then it is translated to a cipher key using the same Hash function as the encryption phase. Finally, the corresponding general decryption algorithms use the cipher key to get back the encrypted message.



(a) Encryption phase



(b) Decryption phase

Figure 1. Framework of the proposed cryptosystem

3. Feature Extraction

We use the preprocessing method described in [12] to localize and normalize the iris. Considering that the upper eyelid, the lower eyelid and the eyelash often cover the iris, we define a region of interesting (ROI) as the inner 3/4 part of the lower half of an iris, which contains enough information to distinguish different irises [13]. We then normalize the ROI into a rectangular block of 256 × 64 pixels (shown in Fig. 2).

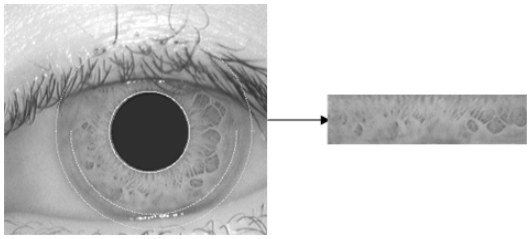


Figure 2. Preprocessing of iris

A 2-D real Gabor filter is defined as following:

$$G(x,y,\theta)=\frac{1}{2\pi\alpha\beta}e^{-(x'^2/2\alpha^2)-(y'^2/2\beta^2)}\cdot\cos(2\pi fx') \quad (1)$$

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\begin{bmatrix}\cos\theta & \sin\theta\\-\sin\theta & \cos\theta\end{bmatrix}\cdot\begin{bmatrix}x\\y\end{bmatrix} \quad (2)$$

Where f is the frequency of the sinusoidal plane wave, α and β are the space constants of the Gaussian envelope along x' and y' axis respectively, θ denotes the orientation of Gabor filter.

The normalized iris image is filtered by a set of 2-D real Gabor filters with θ = 0, 45, 90 and 135 degree. Some examples of the filtered image are shown in Fig. 3. And then each filtered image is equally divided into 16×4 blocks. And for each block, the mean is computed. That is, we can get 16×4×4 = 256 values from an iris image to form a 256-D iris vector. Because of some uncertain factors such as noise, distortion, eyelashes and eyelids occlusion, etc, the different images from the same iris are not exactly identical. Therefore, the iris vectors of these images should be some what different. We can normalize each component of the iris vectors to an integer in the range [0, 15] to remove the most difference. The normalized vector, called iris feature vector, is represented as following:

$$V=(M_1,M_2,\ldots,M_{256}) \quad (3)$$

However, the normalization can not remove all of the difference between the iris feature vectors computed from the images of the same iris and there are still some components of the feature vectors are different. If the number of the different components of two iris feature vectors is less than a threshold T, they are regarded as the ones computed from the images of the same iris. Otherwise, they are regarded as the ones computed from the images of the different iris.

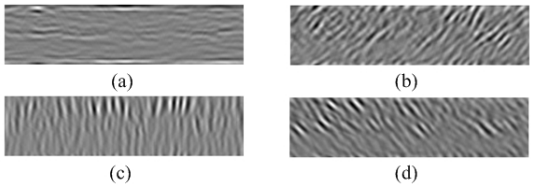


Figure 3. Filtered images

4. Encryption and Decryption

The iris feature vector is used to generate a cipher key for encryption and decryption.

In encryption phase, the feature vector of an iris is used to encrypt the message. Supposed that the length of the iris vector is N (256 in our experiments) and the difference threshold of the feature vectors from the same iris is T, we conduct the following steps to encrypt the message:

1) Compute the Reed-Solomon codes (N+2T, N, T) of the feature vector. Reed-Solomon codes usually contain two parts: vector data and

correction codes. We only keep the correction codes as our error-correct-code (ECC).

2) Translating the feature vector into a fix length iris key (HC) using a Hash function (e.g. MD5).
3) Encrypting the message employing the iris key and some general symmetrical encryption algorithms (e.g. AES).

In decryption phase, the feature vector of an iris is used to decrypt the secret message. The decryption procedure is listed as following:

1) Using the standard Reed-Solomon decoding algorithm to correct the iris vector with the ECC.
2) Translating the corrected vector into an iris key (HC) using the same Hash function with the encryption phase.
3) Decrypting the message using this iris key and the corresponding general decryption algorithms (e.g. AES).

If the decryption vector has a difference less than T with encryption iris, which means that these two vectors are computed from the images of the same iris, the Reed-Solomon decoding algorithm can translate it to the same one with the encryption vector and the decryption should be successful. Otherwise, the decryption fails.

To eliminate the rotation of the iris image, we translate the normalized images 7 times (-6, -4, -2, 0, 2, 4 and 6 pixels), and use each translated one to decrypt the message until success.

5. Experimental Results and Analysis

To test the performance of our method, we use the public database CASIA 1.0 [14], which includes 108 different irises and each iris has seven images with 320×280 pixels in 256 gray levels. Because some of the pictures are defocused, motion blurred, or occluded by eyelids and eyelashes, we choose three images of each iris for experiments, in which two images are used for training, and the other for test. So, we have conducted altogether 108 (108×1) genuine decryptions and 11556 (108×107) imposter decryptions. Fig. 4 shows the result of the FAR and FRR Curves of our experiment. Table 1 lists some typical FAR/FRR and corresponding threshold.

To prevent the impostor from successfully decrypting the data, the FAR should be 0. According to Fig. 5 and Table 1, the error number can be chosen as 107 and the corresponding FAR, FRR are 0%, 5.5556%. According to the theory of Reed-Solomon code, we can choose (570, 256, 107) RS codes for error-correcting in our system.

The possibility to recover the iris key from the ECC without the genuine iris can be computed as following:

$$p = \frac{\sum_{i=0}^{107} \left(15^i \times C_{256}^i\right)}{16^{256}} \approx 2^{-360} \quad (4)$$

That is, the security of this system is similar with that of a cipher key with 360 bits, which is much better than Hao's method (44 bits) [7].

The FRR of our system is nearly 6%, which means that 6% genuine users have to present their iris more than one time for decryption, which still can be accepted.

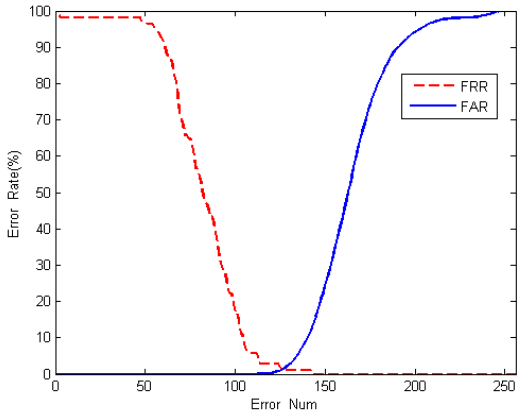


Figure 4. FAR and FRR Curves

Table 1. Typical FAR, FRR and Thresholds

Threshold	FAR(%)	FRR(%)
103	0	11.111
104	0	8.3333
105	0	6.4815
106	0	6.4815
107	0	5.5556
108	0	5.5556
109	0	5.5556
110	0	5.5556
111	0	5.5556
112	0.0087	3.7037
113	0.0173	2.7778

6. Conclusions and Future Work

This paper proposed a novel cryptosystem based on iris key generation. The system extracted quantified vector feature from iris and used Reed-Solomon error-correcting algorithm and Hash function to generate the cipher key for encryption and decryption. Experimental results show that the proposed cryptosystem can work effectively.

In the future, we will test the proposed system on a large database and devise more effective feature extraction algorithm for this cryptosystem.

Acknowledgment

Portions of the research in this paper use the CASIA iris image database collected by Institute of Automation, Chinese Academy of Sciences. This work was supported by a grant from the National High Technology Research and Development Program of China (863 Program) (No. 2007AA01Z195), the Natural Science Foundation of Hei Longjiang Province of China (No. F2007-04) and the Development Program for Outstanding Young Teachers in Harbin Institute of Technology.

References

[1] C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy, and B. V. K. Vijaya Kumar, "Biometric encryption using image processing", *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II*, vol. 3314, pp. 178-188, 1998.

[2] T. C. Clancy, N. Kiyavash and D. J. Lin, "Secure smartcard-based fingerprint authentication", *Proc. ACM SIGMM Multimedia, Biometrics Methods and Applications Workshop, pp*. 45-52, 2003

[3] S. Yang, I. Verbauwhede, "Automatic secure fngerprint verification system based on fuzzy vault scheme", *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, pp. 609-612, 2005

[4] U. Uludag, S. Pankanti and A. K. Jain, "Fuzzy vault for fingerprints", *Proc. of Audio and Video based Biometric Person Authentication*, pp. 310–319, 2005

[5] G. I. Davida, Y. Frankel and B. J. Matt, "On enabling secure applications through on-line biometric identification", *Proc. 1998 IEEE Symposium on Privacy and Security*, pp. 148-157, 1998

[6] G.I. Davida, Y. Frankel, B.J. Matt, and R. Peralta, "On the Relation of Error Correction and Cryptography to an Off Line Biometrics Based Identification Scheme", *Proc. Workshop Coding and Cryptography*, pp. 129-138, 1999

[7] F. Hao, R. Anderson and J. Daugman, "Combining Crypto with Biometrics Effectively", *IEEE Transactions on Computers*, pp. 1081-1088, 2006

[8] A. Goh and D.C. L. Ngo, "Computation of Cryptographic Keys from Face Biometrics," *Proc. Int'l Federation for Information Processing 2003*, pp. 1-13, 2003

[9] F. Monrose, M.K. Reiter, Q. Li, and S. Wetzel, "Cryptographic Key Generation from Voice", *Proc. 2001 IEEE Symp. Security and Privacy*, pp. 202-213, 2001

[10] F. Hao and C.W. Chan, "Private Key Generation from On-Line Handwritten Signatures," *Information Management & Computer Security*, vol. 10, no. 2, pp. 159-164, 2002

[11] X. Wu, D. Zhang, and K. Wang, "A Palmprint Cryptosystem", *International Conference on Biometrics*, pp. 1035-1042, 2007

[12] J.G. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol.15, no.11, pp. 1148-1161, 1993

[13] Li Yu, David Zhang and Kuanquan Wang, "The relative distance of key point based iris recognition", *Pattern Recognition*, pp. 423–430, 2007

[14] CASIA Iris Image Database. {http://www.cbsr.ia.ac.cn/IrisDatabase.htm }