An Iris Cryptosystem for Information Security

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

Securing information is a key issue in the field of network security and cryptography is one of the most effective ways to enhance information security. Biometric cryptography is a technique using biometric features to encrypt the 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 this system, a 256-dimension textural feature vector is extracted from the preprocessed iris image by using a set of 2-D Gabor filters. And then a modified fuzzy vault algorithm is employed to encrypt and decrypt the data. Experimental results demonstrate the feasibility of the proposed system.

1. Introduction

Nowadays, more and more information is transferred through network and how to secure information has become a challenge issue in the field of network security. Cryptography is one of the most effective ways to enhance information security. The traditional cryptographic algorithms (AES, DES and RSA etc.), which encrypt information using cipher keys, are faced with some security problems. 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 for use, which can be stolen or lost. Biometric cryptography [1], which uses biometric features to encrypt the information, can overcome these problems. Currently, some biometric cryptographic algorithms have been developed based on fingerprints [2-4], iris [5-7], face [8], voice [9], signature [10] and palmprints [11] etc.

Among the common biometric features, iris is the most accurate one 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 iris cryptosystem based on iris textural features and a modified fuzzy vault algorithm, which have been used successfully in the fingerprint cryptography [12, 13].

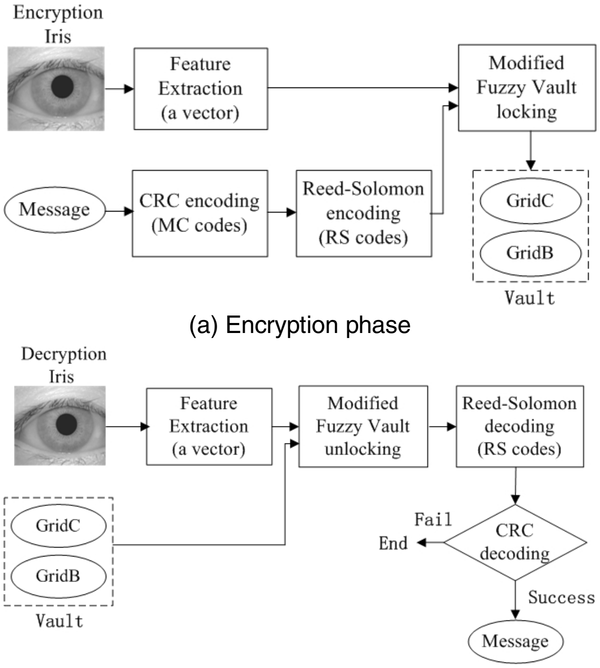
2. Framework of the Proposed System

Fig. 1 shows the frameworks of our system. The message to be secured can be any critical data, for example, cipher keys of traditional cryptosystems.

During the encryption phase, the Cyclic Redundancy Check (CRC) codes of the message is firstly created and appended to the original message to form the mixed codes (MC). Then, the MC codes are encoded to form a RS codes using Reed-Solomon coding algorithm. After that, a textural feature vector (FV) is extracted from the encryption iris. Finally, by using a modified fuzzy vault locking algorithm, the FV is employed to lock the RS codes in a vault composed of two grids (named GirdB and GridC).We only keep the vault, while other information are discarded.

978-0-7695-3278-3/08 $25.00 © 2008 IEEE
DOI 10.1109/IIH-MSP.2008.83

When decrypting, we extract a textural feature vector from the decryption iris to unlock the vault by using a modified fuzzy vault unlocking algorithm. And then, the standard Reed-Solomon decoding algorithm is used to get back the message and its CRC codes. Finally, we check the message with the CRC codes to judge whether the decryption is successful or not.


Encryption Iris
Feature Extraction (a vector)
Modified Fuzzy Vault locking
Message
CRC encoding (MC codes)
Reed-Solomon encoding (RS codes)
GridC
GridB
Vault
Decryption Iris
Feature Extraction (a vector)
Modified Fuzzy Vault unlocking
Reed-Solomon decoding (RS codes)
GridC
GridB
Vault
Fail
End
CRC decoding
Success
Message

(a) Encryption phase

(B) Decryption phase

Fig. 1 Framework of iris cryptosystem

3. Feature Extraction

We use the preprocessing method described in [14] 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 [15]. We then normalize the ROI into a rectangular block of 256 × 64 pixels (shown in Fig. 2).

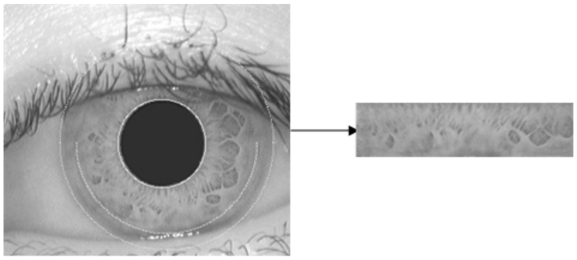


Fig. 2 Preprocessing of iris

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 $\theta = 0^\circ, 45^\circ, 90^\circ$ and 135°. 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. After normalizing each value to an integer in the range [0, 255], we can get a 256-D feature vector:

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

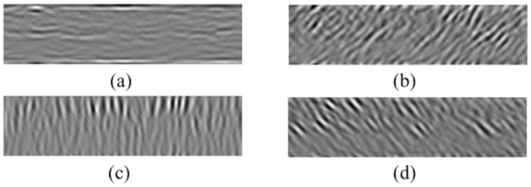


Fig. 3 Filtered images

4. Encryption and Decryption

4.1. Encryption

After having gotten the vector of an iris, we can use the modified fuzzy vault locking algorithm [13] to encrypt the data. There are four key steps in the encryption phase:

1) Compute the CRC codes of the message and append it to the message to form MC codes.
2) Employ RS encoding algorithm to transfer the MC codes to get RS codes with length 256.
3) Create a grid of 256×3, called GridC, and put each element of the RS codes randomly into GridC, following the rule that the *i*th element of RS codes be placed in the *i*th row of GridC. Then fill the rest of GridC with random numbers in an appropriate range to confuse the genuine data.
4) Create another grid of 256×3, called GridB, and put each component of the iris feature vector into GridB, making sure that the order coincides with that of the RS codes in GridC. Then, fill GridB in a way that each row becomes an

arithmetic progression of distance equal to the tolerance value, which is designed to eliminate the differences of vectors extracted from similar images of the same iris. Extra experimental results show that it is suitable to choose the tolerance value as 16.

The GridB and GridC are called a vault. And we only keep vault and discard any other information. Fig.4 shows an example of the encryption process.

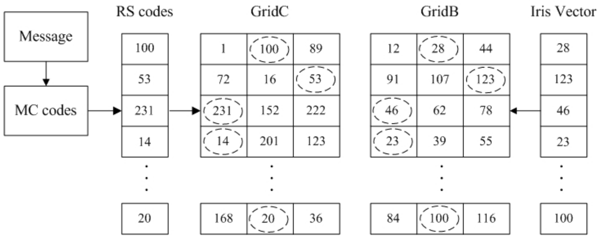


Fig. 4 An example of the encryption process

4.2. Decryption

When decrypting, we only need to know the correct order of the legitimate elements in GridC. The main steps to decrypt the information are listed as following [13]:

1) Extract the feature vector from the decryption iris.
2) Find out an order from GridB by selecting the elements in each row which is nearest to the corresponding element of the decryption vector.
3) Get the RS codes from GridC according to the order in Step 2;
4) Employ the standard RS decoding algorithm to get back the MC codes.
5) Divide the MC codes into two parts: message and CRC codes and check the message using CRC code to judge the decryption success or failure.

In order to eliminate the rotation caused during iris images collection, we translate the normalized images 7 times (-6, -4, -2, 0, 2, 4 and 6 pixels), and use each translated one to decrypt.

The decryption process can deal with the errors resulted from the difference between the genuine irises of encryption and decryption phase. For two vectors extracted from similar images of the same iris, the differences between most of their corresponding elements are less than the vault tolerance, which can be removed by Step 2. The differences of other corresponding elements which are bigger than the tolerance can be handled by using Reed-Solomon coding algorithm (Step 4).

5. Experimental Results and Analysis

To test the performance of our method, we use the public database CASIA Version 1.0 [16], 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 11,556 (108×107) imposter decryptions. Fig. 5 shows the FAR and FRR Curves of this system with different error number which can be corrected by RS coding algorithm. Table 1 lists some typical FAR/FRR, the corresponding error number and the length of the MC codes.

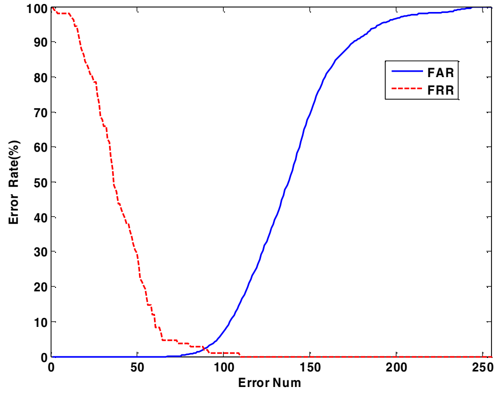


Fig. 5 FAR and FRR curves

Table 1 Typical FAR, FRR and error number

Error Number	MC codes Length	FAR (%)	FRR (%)
62	132	0	8.3333
63	130	0	6.4815
64	128	0	4.6296
65	126	0	4.6296
66	124	0	4.6296
67	122	0.0087	4.6296
68	120	0.0173	4.6296

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 64 and the corresponding FAR, FRR and the length of the MC codes are 0%, 4.6296%, and 128. According to the theory of Reed-Solomon code, we can choose (256, 128, 64) RS codes for error-correcting in our system.

The possibility to recover the message from the vault without the genuine iris can be computed as following:

$$p = \frac{\sum_{i=0}^{64}(2^i \times C_{256}^i)}{3^{256}} \approx 2^{-137} \tag{4}$$

That is, the security of this system is similar with that of a cipher key with 137 bits, which is much better than Hao's method (44 bits) [7].

The FRR of our system is nearly 5%, which means that 5% genuine users have to present their iris more than one time for decryption. This may bring some inconvenience, but it still can be accepted.

6. Conclusions and Future Work

This paper proposed a novel iris cryptosystem. The system extracted vector feature from iris and used the modified fuzzy vault algorithm to encrypt and decrypt messages. Experimental results show that the proposed iris cryptosystem can work effectively, and it is almost impossible to be cracked.

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

Acknowledgement

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] U. Uludag, S. Pankanti, S. Prabhakar and A. Jain, "Biometric Cryptosystems: Issues and Challenges", *Proc. IEEE*, vol. 92, no. 6, pp. 948-960, 2004..

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

[3] S. Yang and I. Verbauwhede, "Automatic secure fingerprint 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. Ngo, "Computation of Cryptographic Keys from Face Biometrics," *Proc. Int'l Federation for Information Processing 2003*, pp. 1-13, 2003

[9] F. Monrose, M. 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. 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] A. Juels and M. Sudan, "A Fuzzy Vault Scheme", *Proc. IEEE Int'l Symp. Information Theory*, pp. 408-421, 2002

[13] A. Nagar, S. Chaudhury, "Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme", *Proc. International conference on Patten Recognition*, pp. 537-540, 2006

[14] J. 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

[15] L. Yu, D. Zhang and K. Wang, "The relative distance of key point based iris recognition", *Pattern Recognition*, pp. 423–430, 2007

[16] CASIA Iris Image Database. {http://www.sinobiometrics.com}