Two Schemes Of Finger Vein Cryptosystem

Gesi Meng, Peiyu Fang
School of Computer Science and Technology
Beijing University of Posts and Telecommunications
Beijing, China
{menggesi, fangpeiyu}@bupt.edu.cn

***Abstract*—Biometric Authentication Technology is an important means to guarantee information security. As one of the most important technology of authentication, finger vein recognition attracts our attention because of its high security, reliable accuracy and excellent performance. However, in the current system, the user's feature vectors are saved in the database directly which would cause a lot of security problems. In order to solve these problems, we designed two complete finger vein encryption schemes based on fuzzy fault and fuzzy extraction. Through experiments, we proved that these two schemes not only guarantee a low False Acceptance Rate but also protect the biometric vectors.**

Keywords—authentication; finger vein; fuzzy vault; fuzzy extraction; security

I. INTRODUCTION

With the rapid development of the Internet, the web information has grown explosively. In order to ensure the security of these information, we need to check individual identity in most fields. Currently the biometric recognition [1] is the most popular authentication technology which has four steps: capturing image, processing image, extracting feature and verifying identity. But in the final step, user's biometric vectors are saved in the database directly, which leads to lots of security vulnerabilities. With the propose of Key Binding System [2] and Key Generating System [3], the researchers apply these methods in fingerprint, face and iris field. However, most of them still stay in the theoretical stage, only a minority put forward specific plans but just ended with undesirable results. Finger vein, as a relative new biometric feature of living body, can overcome these shortcomings. It can be captured easily and contains rich texture information. Therefore, this paper mainly studied the biometric encryption technology and proposed two complete finger vein encryption schemes. Compared with the former biometric encryption systems, main works of this paper are as follows:

- We overcame the weakness in traditional thinning methods and raised an improved approach which removed redundancy point at the bifurcation.
- We designed a finger vein encryption scheme based on fuzzy vault.
- We designed a finger vein encryption scheme based on fuzzy extraction creatively.
- By analyzing the results of experiments, we compared these two schemes and analyzed the security of them.

II. RELATED WORKS

Biometric recognition is a very attractive technique to replace traditional authentication technologies. The main challenge is to provide a secure storage of the biometric vectors [4]. At present, biometric encryption technology is divided into two categories according to the process of generating key. One is Key Binding System, the other is Key Generation System. In recent years, Fuzzy Vault, as a Key Binding System, is a typical method which was proposed by Juels and Sudan [5] in 2002. The most important characteristic of this method is fuzzy which break down the biggest obstacle between the inherent fuzziness of biometry and the accuracy of cryptography. Clancy and Boult [6] proposed secure fingerprint authentication system based on fuzzy vault scheme, they reached 69 bits keys with 20%~30% False Acceptance Rate(FAR). To reduce the FAR, Li and Hu [7] proposed a security-enhanced fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structure. Also Lu and Teoh [8] presented a fuzzy vault scheme in palmprint field, they calculated the proper encrypted polynomial form with row-alone and roe-co-occurrence. Above mentioned schemes are based on the combination between biometry and external keys, which poses a potential security risk while this combination is not ideal. Once the key is lost, the system will collapse. Based on the above analysis, Key Generation System was proposed to avoid external keys. Dodis [9] explained how to extract uniform distribution strong keys from different biometric features through formal definition. Yang [10] made a preliminary attempt for practical algorithm by extracting keys from fingerprint minutiae which has a good robustness. Zhang [11] designed a fuzzy extractor based on iris authentication scheme, which combines error correcting codes with cryptography. However, Key Generation System is still in a immature stage and there is little research about finger vein in this filed.

III. FUZZY VAULT SCHEME

This section presents the scheme of finger vein encryption based on fuzzy vault, the design of this scheme is shown in *Fig. 1*. In the registration phase, we process the captured image of finger vein to get minutiae. Then we select secret key *K* randomly and construct polynomial by *K*. Next, minutiae are projected onto the polynomial to form genuine set *G* and chaff point set *C* is generated randomly. Finally set *G* and set *C* are mixed together to form the fuzzy vault. In the authentication phase, we get the minutiae from current user's image by the same method as above. Then we compare these

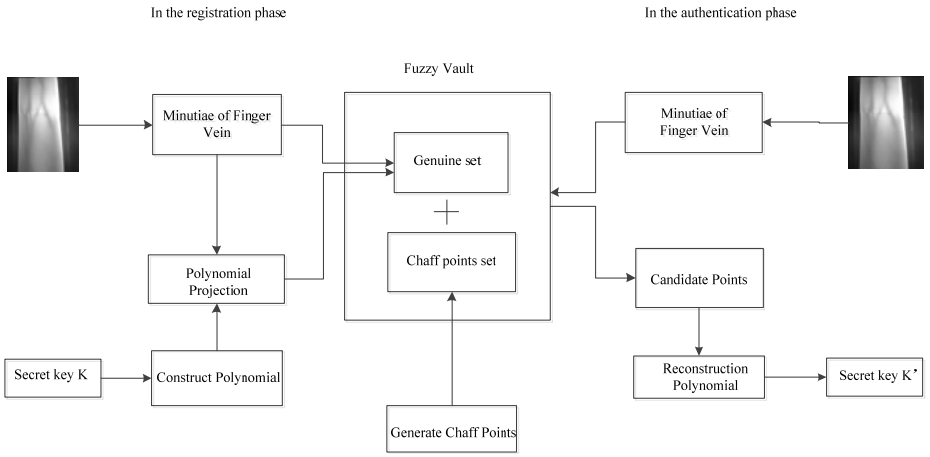


Fig. 1. The scheme of finger vein authentication based on fuzzy vault

minutiae with the points of vault and select some points which may be genuine to form candidate set *T*. Finally we reconstruct the polynomial and restore the secret key K'. If *K* and K' are equal, it is successful to authenticate.

A. Minutiae Extraction

The structure and texture are very important for finger vein image. If texture information is used directly as feature vector, the vector data will be too large to store. We find that, after normalization and skeletonization, there are two kinds of feature points in the image, the first is the intersection, the second is the endpoint. So in this paper, we regard those two kinds of points as minutiae and connect their *X* values and *Y* values to form feature vector. This process is shown in *Fig. 2*.

B. Locking The Vault

The procedure of locking the vault required two input factors: a secret key *K* and minutiae set $M\{(x_i, y_i)\}_{i=1}^{N}$ of finger vein. And the polynomial *P* about *x* is generated by *K*. Then the polynomial is used as the underlying frame to construct the genuine set *G*. In order to hide the set *G*, we generate chaff points set *C* randomly which is far larger than the set *G*. Last, genuine set *G* and chaff point set *C* are mixed together to form

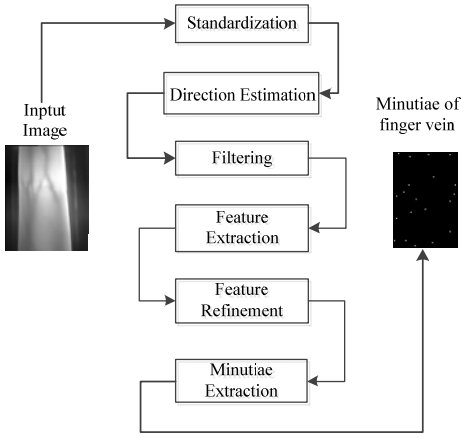


Fig. 2. Extract minutiae of finger vein

the fuzzy vault. The process of locking the vault based on finger vein is as follows.

1) We select a 128-bit key *K* randomly. Then a polynomial *P(x)* is generated by this key. In our scheme, we assign all operations are in a finite field $GF(2^{16})$. So the key *K* is divided into 8 equal segments like $K = f_8 f_7 f_6 ..... f_1$. Then make $f_8, f_7, f_6, ..., f_1$ as the coefficients of polynomial respectively and we get the following polynomial.

$$P(x) = f_8 x^7 + f_7 x^6 + f_5 x^5 + f_4 x^4 + f_3 x^3 + f_2 x^2 + f_1 x + f_0 \quad (1)$$

2) The minutiae set of finger vein is $M\{(x_i, y_i)\}_{i=1}^{N}$, where *N* is the number of extracted minutiae in a finger vein image. Then we connect the values of *x* coordinate and *y* coordinate of each minutia to form a 16-bit number $t_i = [x_i \mid y_i]$. Then it is projected to the polynomial *P* to calculate $P(t_i)$. And genuine set *G* are composed of $(t_i, P(t_i))$, where $i = 1, 2, .., N$.

3) Then N_{chaff} chaff points (x_i', y_i') are generated randomly, where $N_{chaff} >> N$, $i = 1, 2, ..., N_{chaff}$, x_i' is a random number between $\min(t_i)$ and $\max(t_i)$. Similarly, y_i' is a random number between $\min(P(t_i))$ and $\max(P(t_i))$. Moreover, this chaff points (x_i', y_i') does not lie in function curve of polynomial *P*, which means $P(x_i') \neq y_i'$.

4) Genuine set *G* and chaff point set *C* are mixed together to form the fuzzy vault and save it in the database.

C. Unlocking the Fault

In the procedure of unlocking vault, we also need two inputs: minutiae set $M'\{(z_i, w_i)\}_{i=1}^{N}$ and fuzzy vault. The set M' is created by the method shown in *Fig. 2* from current user's finger and vault is gotten from the database. The process of unlocking the vault is as follows.

1) For each point $(t_i, P(t_i))$ in the vault, the 16-bit t_i is split into 8-bit x_i and 8-bit y_i. In order to select the genuine

points, we define a matching box whose center is (z_i, w_i). If some points (x_i, y_i) are located in this box, we regard their corresponding points $(t_i, P(t_i))$ as candidate points. All of these candidate points are formed the set $T = \{t_i, P(t_i)\}$.

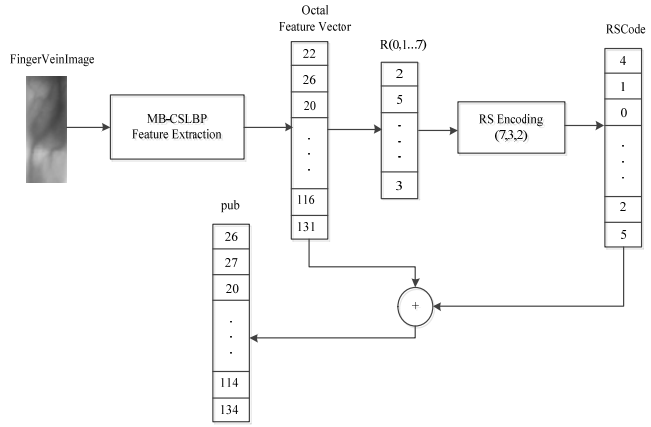
2) If the current user is true, most of points in set T are genuine. So we can select 8 points from T in turn and use these points to calculate the coefficients of polynomial by Lagrange interpolation method [12]. The formula is as follows:

$$P'(x) = \frac{(x-v2)(x-v3)...(x-v8)}{(v1-v2)(v1-v3)...(v1-v8)} p1 + \frac{(x-v1)(x-v3)...(x-v8)}{(v2-v1)(v2-v3)...(v2-v8)} p2 + ... + \frac{(x-v1)(x-v2)...(x-v7)}{(v8-v1)(v8-v2)...(v8-v7)} p8 \quad (2)$$

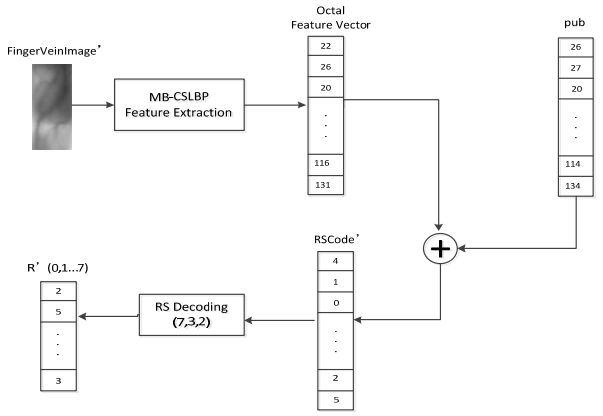
After simplification $P'(x) = c_8 x^7 + c_7 x^6 + ... + c_2 x^1 + c_1$, then $c_8, c_7, ..., c_1$ are connected as a candidate key K'. If $K=K'$, it is successful to restore the key and stop the algorithm. Otherwise choose another 8 points in set T and repeat the above process until the end of set T.

IV. Fuzzy Extraction Scheme

It is difficult to obtain the same finger vein images from one person because our fingers may move or rotation slightly in capture. According to the Digital Communication Systems theory, we regard these variations as additive noises in communication systems. This noise is smaller in the intra-class than in inter-class. And Err Correction Code is used to narrow the differences within intra-class and increase the distance between inter-class so that we can make a good preprocessing for the later identification. Then we choose Reed-Solomon(RS) correcting code [13], a linear block circle code in Information Theory. It has a good capability to correct sudden and random error, which is widely used in digital communication field. So this paper use RS code in finger vein encryption scheme based on fuzzy extraction. The scheme framework is shown in *Fig. 3*.



（a）Encryption



（b）Decryption

Fig. 3. The framework of fuzzy extraction scheme

A. Feature Extraction

Finger vein, as a blood vessel texture, whose length, thickness, structure are valuable texture features. We choose IMC-LBP code [14] which is suitable to describe this type of local texture to extract finger vein features. This algorithm divides the image into many blocks, each of which can be represented by its average gray value. And we only compare the pixel value between the two points whose position is central symmetry so that it has a better feature extraction with both macro and micro information. If the value is greater or equal, set it to 1 otherwise 0. Ultimately they form a 4-dimensional binary vector. By the IMC-LBP algorithm., we finally extract 288 decimal data as feature vector from each finger vein image. This vector not only reflects greater microscopic characteristics of image but also has stronger robustness to noise, which provides good conditions for the subsequent encryption.

B. Finger Vein Encryption

In the encryption phase, the Finger Vein Image (*FVImage*) is captured firstly. Then we extract the feature vector which is defined as Finger Vein Code (*FVCode*). According to the *FVCode*, we calculate two pieces of information: secret information (*R*) and public information (*pub*), which are saved in the database. Then we randomly select *L* numbers from *FVCode* to compose *R*, and encode it by RS code to form a string of numbers defined as *RSCode* in this paper. Finally, *FVCode* and *RSCode* are combined to form *pub*. The formulas are expressed as follows.

Finger Vein Encryption Algorithm

$FVCode \leftarrow FVImage$

$R(0,1..7)^l \leftarrow FVCode$

$RSCode \leftarrow RSEncode(R)$

$pub \leftarrow FVCode \oplus RSCode$

Fig. 4. Finger vein encryption algorithm

C. Finger Vein Decryption

In the decryption phase, the Finger Vein Image' (*FVImage'*) of current user is captured firstly. Then we also get Finger Vein Code' (*FVCode'*) as above. *R* and *pub* are read from database which is saved in the encryption phase. Next, we combine *FVCode'* with *pub* to get *RSCode'* and decode the *RSCode'* to get *R'*. If the Hamming distance [15] between *R'* and *R* is smaller than threshold obtained by training, it is successful to authenticate otherwise failed. Here shows the finger vein decryption algorithm.

Finger Vein Decryption Algorithm

$FVCode' \leftarrow FVImage'$

$RSCode' \leftarrow pub \oplus FVCode'$

$R' \leftarrow RSDecode(RSCode')$

$thresh \leftarrow Hamming(R, R')$

Fig. 5. Finger vein decryption algorithm

V. Experimental Results and Analysis

In our experiment, False Rejection Rate (FRR) and False Recognition Rate (FAR) are the criteria of scheme performance. Those two indicators are inversely related. In practical applications, not only the security is considered but also the practicability. In our system, the FAR is more important than the FRR. We hope that FAR is much lower regardless of higher FRR so that criminal cannot enter the system and ensure the safety of our system.

A. Experimental results and analysis of scheme 1

In this experiment, we used the standard finger vein database. There are 100 images: 10 images for each 10 individuals and the size of each image is 376*328 pixels. After images are processed by the method described in *Fig. 2*, the size of minutiae image is 64*96 pixels. According to the statistics, *N* is 16. Our aim is to prevent attacks in this scheme. So more chaff points means more secure. But when the number of chaff points increases, calculating complexity will increase also. After the compromise, we defined N_{chaff} as 1000. In addition, different sizes of matching box make a big influence on FRR and FAR in the unlocking vault phase, which is shown in the table I.

The experimental results show that when the radius of the matching box is 4, the result is the best, and both FAR and FRR are 0%. The safety of this scheme depends on two factors: whether there are sufficient chaff points and whether the chaff points are fully mixed with genuine points. In this paper, N_{chaff} is defined 1000 and it is much larger than *N*. Also we

TABLE I. THE EXPERIMENTAL RESULT OF SCHEME 1

The Radius of Matching Box	Criteria of Scheme Performance	
	FRR **(%)**	***FAR*** **(%)**
2	0	24.44
4	0	0
6	1.3	0
8	16	6.4

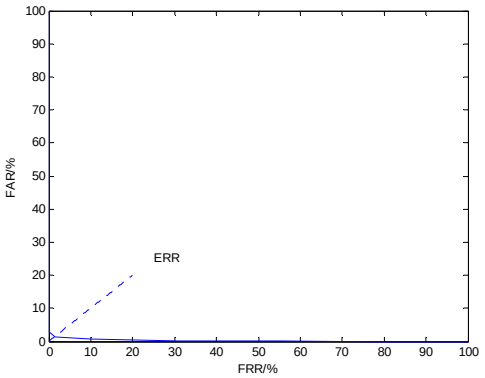


Fig.6. The ROC Curves of Scheme 2

restricted the chaff points within the scope of the genuine set *G* and made them distributed uniformly to protect the genuine points effectively.

B. Experimental results and analysis of scheme 2

In this experiment, we used the standard finger vein database in which the image was obtained through infrared radiation. This database contains 960 different images of 64 persons and each person has 15 finger vein images. Then we got two-dimensional feature vector extracted by the MB-CSLBP method, whose size is 288*960, and the numerical range of this vector is 0~360. In this experiment, we used RS(7,3,2) code. And we randomly extracted 369 data as *R* from the *FVCode*. After *R* was encoded by RS code, we got *RSCode* whose length is 861. Relatively, we selected the former 861 data from *FVCode*, omitting the last three digits, then combined it with *RSCode* to get *pub*.

FAR and FRR were calculated based on the above 960 images, then we got the ROC curve as shown in *Fig. 6*. From this figure, we can conclude that when the threshold value is 0.430, ERR is 1.5%.

C. Comparison Of Two Schemes

We compared the performances of these two schemes shown in the table II and listed their advantages and disadvantages in the table III.

TABLE II . THE PERFORMANCE COMPARISON OF TWO SCHEMES

Performance Comparison	Values of each parameters	
	Fuzzy Vault Scheme	***Fuzzy Extraction Scheme***
FRR	0%	1.504%
FAR	0%	1.429%
time required for each authentication	0.3152s	0.0205s
complexity of force attack	$\frac{2^{16}!}{(2^{16}-128)!}$	2^{2583}
probability of recovering original data	$\frac{1}{C_{1016}^{8} \cdot A_{16}^{8}}$	0
whether external key is required	yes	no

TABLE III . THE ADVANTAGES AND DISADVANTAGES OF TWO SCHEMES

Comparison	Fuzzy Vault Scheme	Fuzzy Extraction Scheme
Advantages	a) High accuracy and ideal FAR. b) The accuracy is relatively stable which only depends on the radius of the matching box. c) It is portable, robust and safe, and the research of this scheme is mature.	a) It does not require external input key to guarantee the high security. b) Faster calculation speed and lower time complexity. c) It has a wide application prospect such as the extracted key can be used in other encryption environment.
Disadvantages	a) Slow calculation speed and high time complexity. b) It requires an external input key which lower the security of scheme.	a) FRR and FAR are not ideal.. b) The accuracy is easily affected by the parameters of RS code.

D. Security Analysis Of Two Schemes

TABLE IV . THE SECURITY ANALYSIS OF TWO SCHEMES

Security Analysis	Fuzzy Vault Scheme	Fuzzy Extraction Scheme
Anti - counterfeiting performance	Different people have different finger vein minutiae image. So they can not use their own images to pretend others. If they attempt to select 8 points randomly to reconstruct polynomial, the probability of success is only $\frac{6136!\bullet 8!}{6144!}$.	The attackers can not get the finger vein feature from database because we save nothing about original data. And different systems have different R and pub, so although one system is attacked, it will not influence other systems.
Re-release performance	When it is needed to update the data in the vault, we can just re-generate the new key during the process of locking the vault.	When it is needed to update the data in the database, users can re-select the R randomly to change their registration information.
Irreversibility	In fuzzy vault, genuine points are hidden in lots of chaff points and they are distributed uniformly, so the key can not be restored directly. Even by force attack, they cannot reconstruct polynomial in short time.	Only R and pub are saved in the database. R contains a few of biological information disorderly and pub is the result of operation. So if attackers get these two parameters, they are unable to restore the original finger vein feature.

VI. CONCLUSIONS

Finger vein, as an evidence of authentication, has a wide application prospects. But currently finger vein authentication system can not protect the feature vector which cause many security risks. In this paper, we designed two finger vein encryption schemes based on fuzzy vault and fuzzy extraction. Finally, experiments verify the effectiveness of these two schemes, and both of them have anti-counterfeiting, re-release and irreversible performance which can prevent criminals attacks. This research lays the foundation for future research in finger vein field.

In future work, we will evaluate our proposed schemes with regard to various input finger vein images.

References

[1] Zhang D D. Automated biometrics: Technologies and systems[J]. Virtual Reality Technologies & Systems, 2000.

[2] Reiter M K, Stubblebine S G. Method for providing authentication assurance in a key-binding system: US, US6405313[P]. 2002.

[3] Gannett D K. Key generating system[J]. 1976.

[4] Yang S, Verbauwhede I. Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme[C]// IEEE International Conference on Acoustics, Speech, & Signal Processing. IEEE, 2005:609-612.

[5] Juels A, Sudan M. A Fuzzy Vault Scheme[J]. Designs Codes & Cryptography, 2002, 38(2):237-257.

[6] Clancy T C, Kiyavash N, Lin D J. Secure smartcardbased fingerprint authentication[C]// ACM Sigmm Workshop on Biometrics Methods and Applications. ACM, 2003:45--52.

[7] Li C, Hu J. A Security-Enhanced Alignment-Free Fuzzy Vault-Based Fingerprint Cryptosystem Using Pair-Polar Minutiae Structures[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(3):543-555.

[8] Lu L, Teoh A B J. Alignment-free Row-co-occurrence Cancelable Palmprint Fuzzy Vault[J]. Pattern Recognition, 2015, 48(7):2290-2303.

[9] Dodis Y, Ostrovsky R, Reyzin L, et al. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. Technical Report 2003/235, Cryptology ePrint archive, http://eprint.iacr.org, 2006. Previous version appeared at EUROCRYPT 2004[C]// 2004:79--100.

[10] Yang W, Hu J, Wang S, et al. An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures[J]. Pattern Recognition, 2014, 47(3):1309-1320.

[11] Zhang F, Feng D, Sun Z. An Iris Authentication Scheme Based on Fuzzy Extractor[J]. Journal of Computer Research & Development, 2008, 45(6).

[12] Zadorin A. The Analysis of Lagrange Interpolation for Functions with a Boundary Layer Component[J]. Nuclear Fusion, 2015, 53(28):426-432.

[13] Cheng M K, Siegel P H. List-decoding of parity-sharing Reed-Solomon codes in magnetic recording systems[C], 2004:640-644 Vol.2.

[14] Chen M, Peiyu Fang. Quick searching of finger vein features based on E2LSH, 2016

[15] Reddy E S, Ramesh Babu I. Performance of Iris Based Hard Fuzzy Vault[C]// IEEE, International Conference on Computer and Information Technology Workshops. IEEE Computer Society, 2008:248-253.