A Fuzzy Vault Scheme for Ordered Biometrics*

Lifang Wu, Peng Xiao, Songlong Yuan, Siyuan Jiang
School of Electronic Information and Control Engineering,
Beijing University of Technology, Beijing, China
Email: lfwu@bjut.edu.cn, xiaopeng9092@emails.bjut.edu.cn, yuansonglong@163.com, jiajia53830120@sina.com

Chang Wen Chen
Dept of Computer science and Engineering, State University of New York at Buffalo,
Buffalo, New York USA
Emai: chencw@buffalo.edu

Abstract**—The fuzzy vault scheme has recently become popular approaches to biometric template protection. Since the original scheme has been designed to work with unordered biometric features, such a scheme cannot effectively utilize order information. We present in this paper a new fuzzy vault scheme that can effectively utilize the ordered characteristics of biometric features. In this scheme, we develop ordered fuzzy vault encoding and decoding processes in order to utilize the ordered information of the features. This prevents the feature components from cross matching and reduces false acceptance ratio (FAR). Furthermore, the original biometric features (or original template) are transformed into binary features (or secure template) by random transformation. The transformed secure template provides both diversity and revocability. This transform also prevents an adversary from obtaining the original biometric template from the secure template and therefore enhance the secure level of the scheme. Based on the proposed scheme, we design an online authentication application framework implemented using face images. We compare our scheme with two contemporary approaches to verify the effectiveness of this approach. Experimental results show that our scheme is able to achieve an improved performance with several desired properties of an online authentication system.**

Index Terms**—Ordered fuzzy vault scheme, Biometric template protection, random transformation**

I. Introduction

The widespread application of biometrics recognition has brought some new problems related to both privacy and security. Unlike password, biometric template is not changeable when it is compromised. Furthermore, the same biometric template allows cross-matching across databases. The ideal framework is that the biometrics can be used for verification and the privacy of biometrics can be protected. Biometric encryption combines biometric with cryptography, so that the biometrics template can be used for authentication and the privacy and security could be protected. By now the research of biometric encryption focuses on biometric template protection.

An ideal biometric template protection scheme should have the following four properties [1].

1) Diversity: The secure template must not allow cross-matching across databases, thereby ensuring the user's privacy.

2) Revocability: It should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data.

3) Security: It must be computationally hard to obtain the original biometric template from the secure template. This property can prevent an adversary from creating a physical spoof of the biometric trait from a stolen template.

4) Performance: The biometric template protection scheme should not degrade the recognition performance (FAR and FRR (false reject rate)) of the biometric system.

However, most existing approaches have the above properties partially. Some approaches have not the desired diversity and revocability. Some have the desired diversity and revocability, but they have the lower security or performance. There usually is a tradeoff between the good performance and high security. It is indeed very challenging to design a secure and high performance scheme that also meets the requirement in diversity and revocability.

Fuzzy vault scheme is one of the most popular approaches for biometric template protection. It is first proposed by Juels and Sudan [2] based on the secret sharing scheme in cryptography. In such scheme, a polynomial of degree n is generated from the key. Then the polynomial is evaluated using the components of biometrics. These genuine points encode the information of both key and biometrics, and they are helper data. Then a large number of random chaff points are generated to lock the helper data and constitute the fuzzy vault. In the authentication stage, if we could get the n+1 true points, the polynomial could be reconstructed and the key can be recovered correctly. In this scheme, the key is split and distributed into the polynomial. The polynomial is then represented using the helper data, which is

*Preliminary results of this research have been reported at ICCCN 2011 entitled: An Ordered Fuzzy Vault Scheme for Online Authentication.
Manuscript received August 16, 2011; revised October 14, 2011; accepted November 8, 2011.

doi:10.4304/jcm.6.9.682-690

obtained by evaluating the components of biometric feature. Finally, the helper data is embedded among the chaff points to form the fuzzy vault. Therefore, both the key and biometrics in this scheme are considered secure.

According to Prof. Jain and his colleague [3], "the fuzzy vault has been designed to work with biometric features represented as an unordered set." Minutiae in fingerprints are one of the features usually used and it is unordered. The fuzzy vault scheme was first implemented by Clancy for finger print template protection [4]. Unlike fingerprint features which are represented by the coordinates of the minutia points, some important biometric features such as Principal Component Analysis (PCA) coefficients in face biometrics are a set of ordered real numbers [5]. Therefore, it is possible for the PCA coefficients of one user to be crossly matched to the PCA coefficients of other users and hence degrade the performance. To apply fuzzy vault to such biometric features, it is necessary to preserve the order characteristic of the feature in the fuzzy vault.

In this paper, we design a new fuzzy vault scheme for ordered biometrics. The proposed scheme combines the random transformation with fuzzy vault to facilitate desired diversity and revocability. The original biometric features (or original template) are transformed into binary features (or secure template) by random transformation. This transform also prevents an adversary from obtaining the original biometric template from the secure template and therefore enhance the secure level of the scheme. In order to prevent the feature components from cross matching and to reduce FAR, we develop novel ordered fuzzy vault encoding and decoding procedures to preserve the ordered information of feature components.

In summary, the proposed scheme not only provides desired properties in diversity, revocability and security, but also is capable of achieving relatively good performance. Based on the proposed scheme, we design an application framework of online authentication. The authentication includes three participants: the user/client, the database server and the verification server.

In the registration stage, the users provide their username, password and biometrics to the client. The client PC extracts the corresponding order biometric features then generates binary features by random transformation. In the meantime, a key is generated from the password. The ordered fuzzy vault encoding is designed to generate the fuzzy vault from the key and binary features. The username and the fuzzy vault are sent to the database server. The username and the key are sent to the verification server. All the sent data is protected using Digital Signature (DS).

In the authentication stage, the users also provide their username, password and biometrics to the client PC. The client PC extracts features of the biometrics and generates binary features by the procedure same as that in the registration stage. Then it sends username and binary features to the database server and sends the username to the verification server. The database server searches the corresponding fuzzy vault by the username. Then ordered fuzzy vault decoding is designed to recover a key from binary features. And the recovered key is sent to the verification server. The verification server searches the stored key by the username and compares the recovered key and stored key. If two keys are identical, the authentication is successful. Otherwise, the authentication stage is considered failed.

The contributions of our proposed scheme include the following: 1) An ordered fuzzy vault encoding and decoding scheme has been developed that utilizes the ordered characteristics of biometric features and prevents the components from cross matching. It results in reduced FAR; 2) The binary features are obtained from the original biometric features by random transformation, which will enables ordered fuzzy vault to achieve enhanced security level. 3) An online authentication application framework is proposed based on the proposed fuzzy vault scheme.

The remaining parts of this paper are organized as follows: In Section 2, we describe the proposed scheme in detail. In particular we describe how random transformation can be used to generate binary features from original features. Ordered fuzzy vault encoding and decoding are designed to utilize the ordered characteristics of biometric features. In Section 3, we propose an online authentication application framework, which includes three participants: the user/client, the database server and the verification server. In our application, key and fuzzy vault are stored separately in database server and verification server, therefore, it is a more secure application system. In section 4, we illustrate the experimental results as well as the analysis. In Section 5, we present the analysis of the security of the proposed application framework. In Section 6, we review some related work in biometric template protection. Finally, Section 7 concludes this paper with a summary.

II. Related Work

Recently, biometric-based authentication has been studied extensively. The existing biometric template protection approaches can be broadly categorized into transformation-based and biometric cryptosystem. The main idea of transformation-based method is to transform the original biometric template into a new transformed template (or secure template). The transformed templates, instead of the original templates, are stored. The same transformation is applied to the query biometric data for authentication.

Transformation-based methods can be further categorized into salting and non-invertible transform approaches depending on the characteristics of the transformation function. In the case of non-invertible transform, it usually is computationally hard to reconstruct the original template using the transformed template and the key, Ratha et al [6] has proposed irreversible transformation for fingerprint template protection. They irreversibly transform feature position and orientations using Cartesian, polar or surface folding transformation. Feng et al [7] thought most of mapping in Ratha's algorithm can be cracked. In Salting, the transformation is invertible to a large extent, and the key should be kept securely. A typical method of salting is bio-hashing [8]. In Salting, the transformation is invertible to a large extent, and the key should be kept securely. A typical method of salting is bio-hashing [8]. It generates random orthogonal space using a user-specific key. Then biometric features are projected onto the random space using point product. Furthermore, the random binary series can be obtained by thresholding.

The salting and non-invertible transformation approach both can provide the diversity and revocability. But security of salting approaches is related to the security of the key[1], while there is a tradeoff between the security and performance in non-invertible approaches.

Biometric cryptosystems combine biometrics with cryptography through appropriate generation/extraction of biometric-based keys that can be used as revocable representations of identity [9]. They mainly include key binding and key generation approaches. Key generation scheme generates a key from biometrics and stores it instead of the original features. In the authentication stage, a key is generated from the query biometrics using the same method. These two keys are compared for authentication. The problem of key generation is that it is difficult to generate key with high stability and entropy [1].

Key binding approaches bind biometrics with a key together. Typical schemes include fuzzy commitment scheme [10], fuzzy vault scheme [2] and so on. Clancy et al. [4] applied the fuzzy vault scheme to fingerprint biometrics. A combined Secure Sketch and Fuzzy Extractor scheme were proposed by Boyen et al [11], however, with no experiment reported. Li and Chang [12] proposed a quantization method of secure Sketch. Sutcuet et al. [13] proposed the use of sketch for face biometric, which is an error tolerant cryptographic technique. Several researchers have developed improved schemes [14-16] for such applications. By now these fuzzy vault embed the original biometric features in the polynomial, it can not provide diversity and revocability. In order to provide diversity and revocability, several researchers introduced password related random transformation to improve both diversity and revocability [15]. Others implemented fuzzy vault schemes for other biometrics such as face [19-22], palm-print [23] and multi-modality biometrics [17, 18]. All these fuzzy vault schemes have not considered for the ordered features.

As we indicated earlier, an ordered fuzzy vault scheme, when properly designed, is able to overcome several problems in the existing schemes. It is based this motivation that we propose an ordered fuzzy vault scheme for face biometrics, and we combine transformation based algorithm with fuzzy vault for biometric template protection.

III. THE ORDERED FUZZY VAULT SCHEME

In the proposed scheme, we obtain a set of binary features from original ordered biometric features by random transformation. Then, an ordered fuzzy vault encoding and decoding scheme is developed to utilize the order characteristics.

A. Random Transformation

Let's assume that the original biometric feature is $\vec{x} = \{x_1, x_2, \cdots x_N\}$. In this section, the original features will be transformed into random binary features $R = \{r_1, r_2, \cdots r_M\}$.

First, a set of random matrices Q_1, Q_2 ,… Q_M of size L×M are generated from password. Take Q_1 for example, a vector $\vec{d} = \{d_1, d_2, \cdots d_L\}$ can be obtained by the following computation:

$$\vec{d} = [Q_1]\vec{x} , \tag{1}$$

Then a binary bit can be obtained from the corresponding component by thresholding:

$$d\_b_j = \begin{cases} 0 & d_j < \tau \\ 1 & d_j \geq \tau \end{cases} \quad \text{j=1, 2…L} , \tag{2}$$

Where, τ is the threshold. It is computed by averaging all the feature components. Then a binary feature r1 is generated by concatenating all these bits:

$$r_1 = \{d\_b_1, d\_b_2, \cdots d\_b_L\} , \tag{3}$$

Similarly, we can get other binary features from $Q_2 \ldots Q_M$. Finally, we can obtain the secure template $R = \{r_1, r_2, \cdots r_M\}$.

In the following fuzzy vault encoding and decoding, the random binary features instead of the original biometric features are used. It can provide different random binary features for different database from the same original biometric features using different sets of random matrices. The cross-matching across databases can be prevented and the diversity can be provided. By the same idea, if the random features are compromised, we can reissue new ones using another set of random matrices. The revocability can be provided.

B. Ordered Fuzzy Vault Encoding

Here, we have a key K_{CRC} of 144-bit, we describe the encoding scheme in detail in four steps.

Step 1: Generating a polynomial.

K_{CRC} is first truncated into 9 non-overlapped numbers of 16 bits (c0, c1, c2,…c8), we get a polynomial of degree 8.

$$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots c_8 x^8 , \tag{4}$$

Step 2: Obtaining helper data by evaluating polynomial.

We evaluate the polynomial using each component of secure template R and get a helper data set G.

$$G = \{(r_i, f(r_i)), i = 1, 2, \cdots M\} , \tag{5}$$

Step 3: Generating an ordered set of chaff points.

Generating chaff points is needed to ensure that the true data is embedded into chaff points to form fuzzy vault. We generate chaff points by the following rules.

$$\begin{cases} s_j \neq r_i \\ w_j \neq f(s_j) \end{cases} , \tag{6}$$

In this process, we order all the chaff points randomly and obtain an ordered set C of chaff points.

$$C = \{(s_j, w_j),\ j = 1,2,\cdots N_C\}\left(N_C = KM, K >> 1\right), \quad (7)$$

Step 4: Generating fuzzy vault

1) For the i[th] component $(r_i, f(r_i))$ of helper data set G, a random number p is generated uniformly with range of [1, K];

2) Compute the sequential number

$$e = (i-1)K + p, \quad (8)$$

3) Replace the e[th] component (s_e, w_e) of ordered chaff point set C using $(r_i, f(r_i))$.

Repeat the above three sub-steps for all the components of set G. We can get the final fuzzy vault as follows.

$$V = \{(a_k, b_k), k = 1,2,\cdots N_c\}, \quad (9)$$

By this procedure, the feature components are embedded in the fuzzy vault by their order number. It prevents the feature components from crossly matching, and reduces the FAR.

C. Ordered Fuzzy Vault Decoding

Assume that the binary features provided by client PC are $T = \{t_1, t_2, ...t_M\}$.

For i^{th} component t_i of T, we compute the hamming distance between t_i and every components of i^{th} space in the set V.

$$Distance_{i,j} = Dis\_hamming(t_i, a_j),\ j = iK, iK+1, LiK+K-1, \quad (10)$$

Then, we get the number $j\_\min$ corresponding to the minimum Hamming distance.

$$\begin{aligned} Dis_i &= \min\{Distance_{i,j},\ j = iK, iK+1, \cdots iK+K-1\} \\ &= Distance_{i,j\_\min} \qquad i = 1,2,\cdots M \end{aligned}, \quad (11)$$

We then rank these distances Dis_i (i=1,2…M) according to increasing order. Next we choose the first 12 distances. Without loss of generality, suppose these distances are $Dis_1, Dis_2, ..., Dis_{12}$. Then we get the corresponding points $\left\{\left(a_{1\_\min}, b_{1\_\min}\right), \left(a_{2\_\min}, b_{2\_\min}\right), \cdots \left(a_{12\_\min}, b_{12\_\min}\right)\right\}$ from the fuzzy vault V. In theory, 9 true points are needed to construct the polynomial. Therefore, we have *g* cases from the above 12 points $g = C_{12}^9 = 220$.

In general, we can construct the degree 8 polynomial and recover the key from any of 220 cases. In practice, if there is more than one false point in a case, the polynomial reconstruction will usually fail and no key is generated because the false points are random numbers. All the cases that have 9 true points can generate the same key. Therefore, in our scheme, when a key can be generated from any case, we shall skip all the remaining cases and produce the key.

IV. An Online Authentication Application Framework

In this section, we design an online authentication framework based on face biometrics. The application includes client, the database server and the verification server. The application includes both registration and authentication stages. The framework is shown in Fig. 1.

In the registration stage, the users provide their username, password and face image to the client PC. The client PC extracts face features $\vec{x} = \{x_1, x_2, \cdots x_N\}$ using PCA. Then the scheme generates binary features $R = \{r_1, r_2, \cdots r_M\}$ by random transformation. In the meantime, a key of 144 bit is generated from password. The ordered fuzzy vault encoding is used to generate fuzzy vault $\{t_1, t_2, \cdots t_M\}$ from the key and binary features. Then the username and the fuzzy vault are sent to the database server. The username and the key are sent to the verification server. All the data sent to the server should be protected using digital signature. The server receives the corresponding data and checks the data using digital signature. If the data is changed, the server will require the client to resend the data. If the data is not changed, the server will store the corresponding data.

In the authentication stage, users also provide their username, password and face image to the client PC. The client PC extracts features $\{y_1, y_2, \cdots y_N\}$ of face image, and generates binary features $\{t_1, t_2, \cdots t_M\}$ by random transformation. Then it sends username and binary features to the database server and sends the username to the verification server. All the data also is protected using digital signature. The database server obtains the corresponding fuzzy vault by username and make sure that the fuzzy vault has not been changed. Then the database server generated the recovered key using ordered fuzzy vault decoding from the binary features. Then the database server sends the recovered key to the verification server. The verification server chooses the stored key by the username and compares the recovered key and stored key. And it sends the client PC the authentication result. If two keys are identical, the authentication is successful; otherwise, the authentication stage is considered failed.

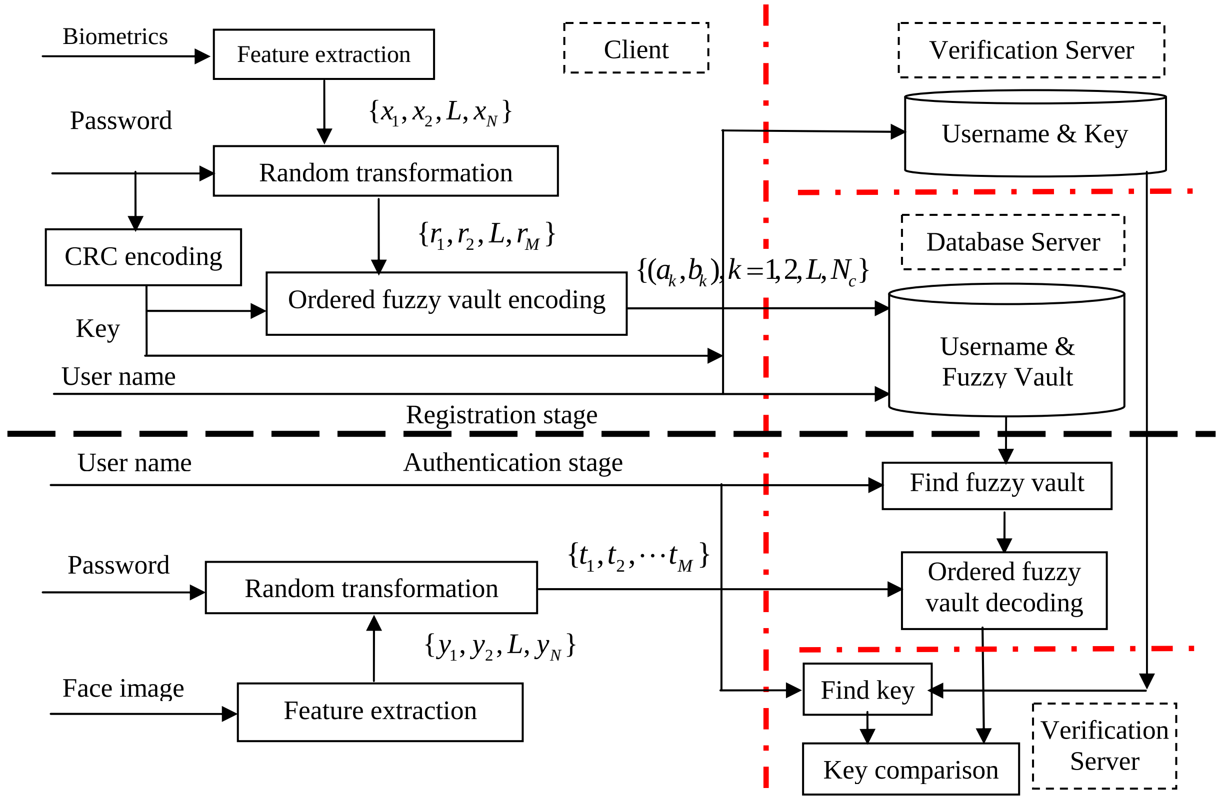

Figure 1. The frame work of online authentication application

A. Feature Extraction

In this research, PCA [5] is used for feature extraction. From all the samples of training set, we can get a covariance matrix U. From this covariance matrix, we can compute the N' eigenvectors of U. Then we rank the eigenvectors according to descending order of corresponding eigenvaules. The first N Eigenvectors are selected as the eigenfaces. $\Psi = \{\psi_1, \psi_2, \cdots \psi_N\}$, These eigenfaces are orthogonal to each other.

Suppose that face image is represented as $\vec{x}$, the corresponding feature vector $\vec{x}$ can be obtained by linear mapping:

$$\vec{x} = \Psi^T(\vec{z} - \overline{z}), \tag{12}$$

Where $\overline{z}$ is the average image of all face images in the training set. By now, a face image $\vec{z}$ can be represented as an original template (or a set of original features). $\vec{x} = \{x_1, x_2, \cdots x_N\}$.

B. Data Protection Using Digital Signature

All the data transmitted from the sender to the receiver should be protected using the digital signature SN, so that the receiver could check the integrity of the transmitted data.

The approach of RSA is implemented to generate digital signature. Let's assume that the transmitted data is *D*. First, the abstract *A* of the *D* is generated from hashing. Then the abstract *A* is encrypted using private key and the signature *SN* is generated. The final data *H* is the union of transmitted data *D* and the signature *SN*.

$$H = D \cup SN, \tag{13}$$

At the receiver side, the integrity of the received data should be checked first. The data *H* is split into data *D* and the signature *SN*. The same hashing is used to generate the abstract A' from *D*. Then the public key is used to decrypt the digital signature SN and obtain the original abstract *A*.

If $A' \neq A$, it means that the data *H* has been changed, the receiver will reject the data and ask the sender to resend the data. Otherwise, the receiver thinks the received data is identical to the sent data.

V. Experiment Results

In this section, we report several experiments for evaluating authentication performance (subsection C) is the same as that in [21]. We also test how the feature number influences the authentication performance (sub-section A). We find that the optimal feature is 25 in our scheme. Then we test variation of FAR and FRR with the ratio K of chaff points number to template number. We find that the FAR decreases and the FRR increases as the K increases. Finally, we compare the performance of our scheme with that using the original face features in the ORL and the FRAV2D face database. The experimental results showed the Equal Error Ratio (EER) of our scheme is 1.35-2.16% higher than that using the original face features. It means that the authentication performance of our scheme degrades a little but the security of our scheme is comparatively high.

We have tested the proposed scheme using the ORL face database [24], which contains 400 face images from 40 subjects with 10 face images each subject. Images of some subjects were taken at different time instances. Some vary with illumination, expression and pose variation. The example images are shown in Fig. 2

Figure 2. The example face images in ORL database

We also test our approach using FRAV2D database [25], in which we choose 1000 face images from 100 subjects with 10 face images each subject. The example face images are shown in Fig. 3.

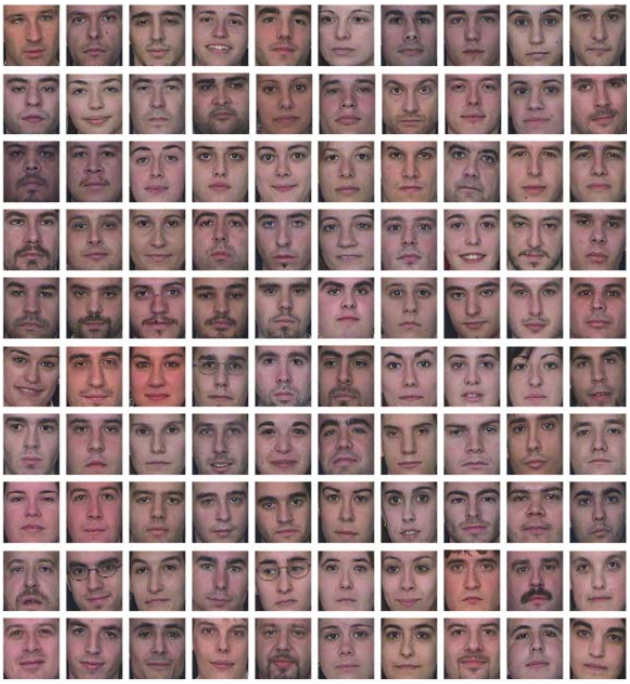

Figure 3. The example face images in FRAV2D database

A. *How Does theFeature Number Influence the Performance*

Let's assume that 160 PCA coefficients are chosen and ordered by their corresponding eigen values. We have the feature vector of 160 dimensions. We choose the first N coefficients and we get the N dimensional feature vector. We test the performance under different N. Fig. 4 shows the Equal Error Ratio (EER) Vs feature number N.

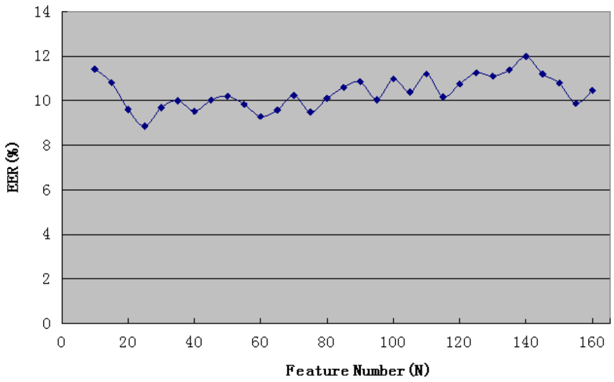

Figure 4. Performance under different feature number N

From Fig. 4 we can see that when we choose the first 25 features (N=25), our approach has the minimum EER. In the following experiments, we compare our approach with Wang's approach [19] under N=20 and with our previous approach [20] under N=55, these two feature numbers are chosen by these two compared approaches.

B. *How Does the K Influence the Performance*

The relationship between K, NC and M is as follows:

$$K = Nc / M \ , \tag{14}$$

When M is determined (M=12), if we change K, the number NC of chaff points will change. We test the performance of our approach under different K. Fig. 5 shows the FAR and FRR with different K under the optimal feature number N=25.

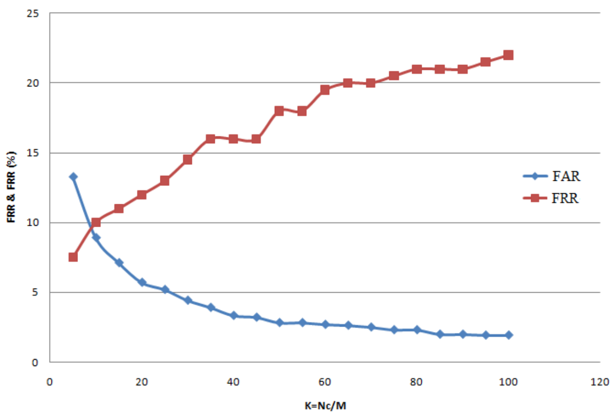

Figure 5. FAR and FRR vs the Ratio K of chaff point number to template number

From Fig. 5 we can see that FRR increases and FAR decreases when K increases, the number of chaff points increase. On the one hand, these chaff points will influence the true points. It will decrease the probability of the genuine subjects are rejected. And it will also cause fewer subjects are falsely accepted. The FAR will be decreased.

C. *Authentication performance*

We compare our approach with the approach reported in [19] and our previous work in Ref [20] respectively.

In the experiments of [19], the first 5 images of each subject are used as training set, the rest are used for testing. The first 20 PCA coefficients are selected for face features (N=20). The number of components in transformed template varies between 12 and 20. For fair comparison, we also implement our experiment using the same parameters as that in [19]. The random transformation in our scheme is related to the same password and the transformation matrices for different subject are same. It is same as the user-independent scenario of experiments in [19]. The experimental results in [19] are shown as EER (Equal error Ratio). We choose the nearest points in authentication stage which is the same as the scenario (w=1) of [19]. The results of comparison for this experiment (EER) are shown in Table I.

TABLE I.
COMPARED EER (%) UNDER DIFFERENT M

M	Approach in [19] (W=1)	Our scheme (N=20)
12	39.75	11.13
13	38.26	10.29
14	35.76	10.07
15	33.5	10.05
16	30	9.98
17	24.01	9.90
18	24.81	9.91
19	20.52	9.75
20	18.52	9.61

From Table I, we can see that our approach is much better than scheme in [19].

We also compare the proposed scheme with our previous approach that was developed just recently [20]. The first 55 PCA coefficients are used for face features. The number of components in transformed template varies 12 through 20. The FAR and FRR are compared in Table 2.

TABLE II.
COMPARISON OF OUR SCHEME WITH SCHEME IN [20]

M	Our scheme (N=55)		Scheme in [20]	
	FAR	FRR	FAR	FRR
12	1.92	21.0	5.26	48.5
13	2.31	19.0	8.27	42.5
14	2.63	17.5	8.14	46.0
15	2.76	17.5	10.06	39.0
16	3.21	17.5	9.81	37.0
17	3.33	16.5	14.23	34.5
18	3.59	16.5	13.01	34.5
19	3.78	17.0	15.13	30.5
20	4.17	15.5	15.38	23.0

From Table II, we can conclude that the proposed scheme also achieves better performance than that in [20] under same parameters. We can also conclude that FAR is substantially lower than FRR. These results prove that the ordered fuzzy vault encoding and decoding scheme is able to significantly reduce FAR because our scheme makes cross matching of different component impossible.

D. Compare the Performance of Our Approach with the Original Face Features

In this section, we compare our approach with that using the original features using two face database ORL face database and FRAV2D face database. The experimental results are shown in Table III.

TABLE III.
COMPARED EER(%) OF OUR APPROACH WITH THAT USING ORIGINAL FEATURES

	Feature Number (N)	ORL	FRAV2D
Our approach	20	9.61	8.655
	25	8.855	8.125
	55	9.835	8.29
Use the original PCA	20	8.105	7.175
	25	7.505	6.555
	55	7.675	6.615

From Table III, we can see that the EER of our approach is higher about 1.35-2.16% than that using the same number of original PCA features. Both approaches obtain the optimal result (the generally EER is minimum) under the feature number of 25. It is consistent with the results in Fig. 4.

VI. SECURITY ANALYSIS

The application includes three participants: the client, the database server and the verification server.

A. Security on the client

In the registration stage, the client receives the username, password and biometrics. It then generates the key and the ordered fuzzy vault and sends them to database server or verification server. In the authentication stage, the client also receives the username, password and biometrics. It then generates the binary features using random transformation. Then it sends the username and the transformed features to the corresponding server. Because the client does not store any data, it is impossible to compromise user's information from it.

B. Security on the database server

In the registration stage, the database server received the username and ordered fuzzy vault from the client and stores them. In the authentication stage, the database server receives the user name and the transformed features. Then it recovers the key from the stored fuzzy vault. The database server stores the fuzzy vault. Therefore, it is possible to crack the fuzzy vault for user's information. But how difficult is it to crack the fuzzy vault ?

We analyze the security of proposed fuzzy vault scheme regarding to brute-force attacks. The security of the fuzzy vault scheme is based on infeasibility of polynomial reconstruction problem. Here we assume that the degree of polynomial is 9. In theory, the attacker needs to guess at least 9 true helper data to pass through authentication. Suppose the attacker know that K is 20. The attacker needs to find a true helper data from 20 data in which case the computation is C_{20}^1. In order to find 9 true data, the total computation will be $(C_{20}^1)^9$. The expected number of combinations that need to be evaluated is equal to $(C_{20}^1)^9 = 5\times10^{11}$. This corresponds to a computational time of 16 years based on our current implementation.. The probability that a combination of points decodes the secret is about equal to $1/(C_{20}^1)^9 = 2\times10^{-12}$.

C. Security on the verification server

The verification server stores only the username and the key. And the key is protected by the digital signature. If the key is changed, it will result in the failing of the authentication. Even if the key is comprimised, the biometric template is still secure.

In summary, in our application framework, the fuzzy vault and key are stored separately in the database server and the verification server. It is difficult for an attacker to compromise password and biometric template at the same time. It is also shown that random transforms are noninvertible by demonstrating that it is computationally as hard to recover the original biometric identifier from a transformed version as by randomly guessing. Therefore, the security of the proposed scheme is high.

VII. Conclusion

In this paper, we have developed an ordered fuzzy vault scheme. The proposed new scheme combines random transformation based approach with fuzzy vault. This new scheme provides the desired diversity and revocability for biometric template protection. As indicated throughout this paper, the ordered characteristics of face features we introduced in this research leads to numerous benefits. Based on this concept, an ordered fuzzy vault encoding and decoding scheme have been developed to implement the proposed approach. Furthermore, by making use of face images, we designed an online authentication application framework. The framework includes three participants: the user/client, the database server and the verification server. Experimental results confirm the effectiveness of the proposed scheme.

The contribution of our proposed scheme include: 1) An ordered fuzzy vault encoding and decoding scheme is developed. This will keep components from cross matching and reduce the FAR. 2) The binary features are obtained from the original face features by random transformation. This transform provides desired diversity and revocability. Furthermore, binary features will protect ordered insertion from reduction in security. 3) Using face biometrics, an online authentication application framework is designed and implemented, which includes user/client, database server and the verification server. In our application, fuzzy vault and key are stored separately. It is more secure.

Acknowledgment

This paper is supported partially by the Beijing municipal Nature Science Foundation under Grant No 4091004 and Beijing Municipal Talent Training Program under Grant No 2009D005015000010.

References

[1] A. K. Jain, K. Nandakumar and A. Nagar, “Biometric Template Security,” EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, pp. 1-20. January 2008.

[2] A. Juels and M. Sudan, “A Fuzzy Vault Scheme,” IEEE International Symposium on Information Theory, pp. 408-426, 2002.

[3] K. Nandakumar, A. K. Jain and S. Pankanti, “Fingerprint-Based Fuzzy Vault: Implementation and Performance,” IEEE Trans. On Info. Fore. And Security, 2(4), pp. 744-757, Dec 2007.

[4] T. Charles Clancy, N. Kiyavash and D. J. Lin, “Secure smartcard-based fingerprint authentication,” Proc. ACMSIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop, pp. 45-52, 2003.

[5] M. Turk and A. Pentland, “Eigenfaces for recognition,” Journal of Cognitive Neuroscience 3 (1), pp.71–86, 1991.

[6] N. Ratha, S. Chikkerur, J. Connell, R. Bolle, Generating Cancelable Fingerprint Templates, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, pp. 561-752, 2007.

[7] Feng Quan, Su Fei Cai Anni and Zhao Feifei, “Cracking Cancelable Fingerprint Template of Ratha”, 2008 International Symposium on Computer Science and Computational Technology, pp. 572-575, Dec 2008.

[8] A. B. J. Teoh, A. Goh, and D. C. L Ngo, “Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs,” IEEE Transactions on Patt. Ana. and Mac. Intel. 28(12), pp. 1892-1901, Dec, 2006.

[9] S. Jassim, H. Al-Assam, and H. Sellahewa, “ Improving Performance and Security of Biometrics Using Efficient and Stabble Random Projection Techniques,” Proceedings of the 6th International Symposium on Image and Signal Processing and Analysis (2009), pp. 556-561, 2009.

[10] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” Sixth ACM Conf. on Comp. and Comm. Security, pp. 28-36, 1999.

[11] B. Xavier, D. Yevgeniy, K. Jonathan, R. Ostrovsky and A. Smith, “Secure remote authentication using biometric data,” In Proc. of Advances in Cryptology 24th Annual International Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005). Springer-Verlag, pp. 147-163, 2005.

[12] Q. M. Li and E. C. Chang, “Robust, short and sensitive authentication tags using secure sketch,” in Proceedings of the 8th Multimedia and Security Workshop (MM and Sec '06), pp. 56-61, 2006.

[13] Y. Sutcuet, Q. M. Li and N. Memon, “Protecting biometric template with sketch: theory and practice,” IEEE Transactions on Information Forensics and Security, 2(3) Part 2, pp. 503-512, 2007.

[14] P. Li, X. Yang, K. Cao, X. Q. Tao, R. F. Wang and J. Tian, “An alignment-free fingerprint cryptosystem based on fuzzy vault scheme,” Journal of Network and Computer Applications, 33(3), pp. 207-220. May 2010.

[15] K. Nandakumar, A. ek and A. K. Jain, “Hardening Fingerprint Fuzzy Vault Using Password,” ICB 2007, pp. 927-937. 2007.

[16] D. S. Moon, W. Y. Choi and K. Y. Moon, “Fuzzy Fingerprint Vault using Multiple Polynomials,” The 13th IEEE international Symposium on Consumer Electronics (ISCE2009), pp. 290-293, 2009.
[17] K. Nandakumar and A. K. Jain, “Multi-biometric Template Security Using Fuzzy Vault,” 2nd IEEE International Conference on Digital Object Identifier, pp. 1 - 6, 2008.
[18] E. J. C. Kelkboom, X. Zhou, J. Breebaart, R. N. J Veldhuis, C. Busch, “Multi-Alogrithm Fusion with Template Protection,” IEEE 3rd International Conference on Digital Object Identifier, pp. 1- 8, 2009.
[19] Y. J. Wang and K. N. Plataniotis, “Fuzzy vault for face based cryptographic key generation,” 2007 Biometrics Symposium, pp. 1 – 6, 11-13 Sept. 2007.
[20] L. F. Wu and S. L. Yuan, “A face based fuzzy vault scheme for secure online authentication,” Proc. on International Symposium on Data Privacy and E-commerce ISDPE 2010. Buffalo NY USA, pp. 45-49, Sep 13-15 2010.
[21] L. F. Wu, S. L. Yuan, P. Xiao, and C. W. Chen, “An ordered biometrics based fuzzy vault scheme for online authentication,” International Conference on Computer Communication Networks, ICCCN 2011.
[22] Y. C. Feng, P. C. Yuen and A. K. Jain, “A Hybrid approach for face template protection,” Biometric Technology for Human Identification V. Proceedings of the SPIE, Volume 6944, pp. 8-11, 2008.
[23] D. Zhang, W. K. Kong, J. You, and M. Wong, “Online PalmPrint Identification,” IEEE Trans. PAMI, vol. 25, no. 9, pp. 1041-1050, 2003.
[24] http://www.cl.cam.ac.uk/research/dtg/attarchive/facedata-base.html.
[25] http://www.frav.es/databases/FRAV2d/.

Dr Lifang Wu received the B.S degree in electronic engineering, M.S. degree in material engineering and Ph.D. degree in pattern recognition and intelligent system from Beijing University of Technology, Beijing, in 1991, 1994 and 2003 respectively. She is presently Professor of Electronic Engineering at the Beijing University of Technology (BJUT). Her research interests are in the areas of biometric encryption, face detection and recognition and digital image/video analysis. She is co-author of about 10 journal papers and 30 conference papers.
Dr. Wu is a Member of Chinese Institute of Electronics (CIE). She is also an editor of Signal Process of China. She is a session chair of ACM ICIMCS 2010.

Mr Peng Xiao received the B.S. degree in Electronic and information Engineering from North China Institute of Science and Technology, Hebei, P.R. China, in 2009. He is pursuing a Master degree in the School of Electronic Information and Controlling Engineering at Beijing University of Technology. His research interests include face encryption and face recognition.

Mr Songlong Yuan received the B.S. degree in Electronic Engineering from Yichun University, Jiangxi, P.R. China, in 2006. He received his M.S. degree in Information and communication engineering from Beijing University of Technology, Beijing, in 2011. His research interests include biometric encryption , data privacy and face recognition.

Ms Siyuan Jiang received the B.S. degree in Micro-electronics from Chongqing University of post and telecommunication, Chongqing, P.R. China, in 2009. She is pursuing a Master degree in the School of Electronic Information and Controlling Engineering at Beijing University of Technology. His research interests include face encryption and face recognition.

Dr Chang Wen Chen has been a Professor of Computer Science and Engineering at the University at Buffalo, State University of New York, since 2008. Previously, he was Allen S. Henry Distinguished Professor in the Department of Electrical and Computer Engineering, Florida Institute of Technology, from 2003 to 2007. He was on the faculty of Electrical and Computer Engineering at the University of Missouri - Columbia from 1996 to 2003 and at the University of Rochester, Rochester, NY, from 1992 to 1996. From 2000 to 2002, he served as the Head of the Interactive Media Group at the David Sarnoff Research Laboratories, Princeton, NJ. He has also consulted with Kodak Research Labs, Microsoft Research, Mitsubishi Electric Research Labs, NASA Goddard Space Flight Center, and Air Force Rome Laboratories.
Dr Chen received his B.S. from University of Science and Technology of China in 1983, MSEE from University of Southern California in 1986, and Ph.D. from University of Illinois at Urbana-Champaign in 1992. He was elected an IEEE Fellow for his contributions in digital image and video processing, analysis, and communications and an SPIE Fellow for his contributions in electronic imaging and visual communications.
Dr. Chen has been the Editor-in-Chief for IEEE Trans. Circuits and Systems for Video Technology (CSVT) from January 2006 to December 2009. He has served as an Editor for Proceedings of IEEE, IEEE Trans. Multimedia, IEEE Journal of Selected Areas in Communications, IEEE Multimedia Magazine, Journal of Wireless Communication and Mobile Computing, EUROSIP Journal of Signal Processing: Image Communications, and Journal of Visual Communication and Image Representation. He has also chaired and served in numerous technical program committees for IEEE and other international conferences.