FUZZY VAULT FOR FACE BASED CRYPTOGRAPHIC KEY GENERATION

Yongjin Wang, K.N. Plataniotis

The Edward S. Rogers Sr. Department of Electrical and Computer Engineering,
University of Toronto, 10 King's College Road, Toronto, ON, Canada, M5S 3G4

ABSTRACT

This paper presents a method for changeable cryptographic key generation using face biometrics signal. A previously introduced scheme, *fuzzy vault*, is utilized for secure binding of randomly generated key with extracted biometrics features. The major technical difficulty is to map noisy biometrics representation to the exactly correct key. In this paper, the proposed method is based on 2-dimensional quantization of distance vectors between biometrics features and pairs of random vectors. A windowing process is applied to tolerate the variations of biometrics signals. Further, we also introduce a two-factor scheme, where the quantized distance vectors are generated with user-dependent random vectors. By integrating a second factor, both the biometrics and the key are changeable, and zero error rate can be obtained.

1. INTRODUCTION

Cryptography is an important technique in information security and some related applications, particularly in encryption, authentication, and access control. Traditional cryptographic systems verify the authenticity of an individual based on the possession of a cryptographic key. Due to the large length and randomness of the key (e.g., 128-bit key for AES [1]), a short password is usually used to encrypt the cryptographic key. The user only needs to remember the short password to retrieve the key. By using this method, the cryptographic key has the same level of security as that of the password, which can be forgotten and stolen [2].

Biometrics based authentication systems confirm an individual's identity based on the physiological and/or behavioral characteristics of the individual [3]. It has intrinsic advantages over password based methods. Biometrics based method provides direct link between the service and actual user. With biometrics, there is nothing to lose or forget, and it is relatively difficult to circumvent [2]. Biometrics and cryptography are two most prominent and complementary solutions for user authentication, data integrity preservation, and trustworthy verification. By combining biometrics with cryptography, high level of security can be expected. Effective combination of biometrics with cryptography will have significant contribution to secure data exchange over Internet, and reliable digital right management.

The major technical difficulty in the marriage of biometrics with cryptography is due to the noisy nature of biometrics signal and the exactly correct requirement of cryptographic key. The capability of variation tolerance is of fundamental importance in the design of biometrics based cryptographic systems. Secondly, due to the limited number of biometric traits that human possesses, it is desirable to have changeable biometrics templates such that the users can have different biometrics representations for various application. When the biometrics template in one application is compromised, a new biometrics templates can be issued. Thirdly, the cryptographic key should also be changeable such that distinct keys can be generated for different applications from the same biometrics signal. Fourthly, biometrics signals reflects the user's physiological and/or behavioral characteristics.The user's privacy may be revealed if the storage device is compromised. The biometrics templates should be stored in a format such that the user's privacy is protected even the storage device is compromised.

A few recent research proposals have been introduced to link biometrics with cryptography, the majority of which focus on two biometrics modalities, fingerprints [4-6] and iris [7]. Although many solutions have been suggested, the problem of mapping signals such as face images into unique and robust cryptographic keys presents significant challenges. The objective of this research is to develop a systematic framework for effective combination of biometrics with cryptography to generate changeable keys with privacy preservable and changeable biometrics representation. In this paper, we explore the use of a previously proposed scheme , *fuzzy vault* [8], for cryptographic key generation in a face based authentication scenario. Specifically, we introduce two schemes based on user-independent and user-dependent mappings. The user-independent method utilize the same set of parameters for all users. The user-dependent method is a two factor scheme with distinct parameters for different users. The experimentation shows that the user-dependent scheme is capable of producing zero error rate and changeable biometrics representation.

The remainder of this paper is organized as follows. Section 2 provides a brief review of related works. The details of the proposed methods are presented in Section 3. In section 4, we present the experimental results. Section 5 provides conclusion and future works.

1-4244-1549-7/07/$25.00

2. RELATED WORKS

A number of research works have been reported toward effective combination of biometrics with cryptography. Bodo [9] first proposed to use the data derived from the biometrics templates as the a cryptographic key directly in his German patent. Chang et al [10] introduced a method to map the extracted face features to bits, and the bit stream is used as the cryptographic key. A major problem with their methods [9][10] is that the biometrics data is usually subject to drastic variation, and in general can not produce exactly the same key. Further, neither the biometrics signal nor the key are changeable. If the key is ever compromised, then this biometrics signal is irrevocably lost.

An alternative solution is to randomly generate a cryptographic key, and bind the key with the biometrics features in a way such that neither the biometrics nor the key are revealed even the stored templates are compromised. Juels and Wattenberg [11] proposed a fuzzy commitment scheme to combine the biometrics features with randomly generated keys through a XOR operation. Error correction coding methods are used to tolerance variations of biometrics features. Hao et al [7] implemented a similar scheme in an iris recognition problem. Jeuls et al and Hao et al's methods provides rigorous security, but it is not clear how to produce exactly the same number of bits as the key from face images. Further, the effectiveness of using error correction codes to tolerant large variations, e.g., face images, is yet to be studied.

The fuzzy commitment scheme requires correspondence of features in terms of order. To overcome this problem, Juels and Sudan [8] introduced the fuzzy vault scheme. The hardness of this scheme is based on the difficulty of polynomial reconstruction problem. During enrollment, a user selects a polynomial $f(x)$ and encode his cryptographic key $\mathbf{k}$ into the polynomial's coefficients. The encoding of $\mathbf{k}$ can be achieved by dividing $\mathbf{k}$ into non-overlapping chunks and mapping to the coefficients [12]. For a given set of features $\mathbf{x} \in \Re^N$, the polynomial $f(x)$ can then be evaluated at each element $\mathbf{x}_i$ and store all pairs of $\{(\mathbf{x}_i, f(\mathbf{x}_i)), i = 1...N\}$ as the genuine set G. The user then generate a random set of chaff pairs C, and merge with the G set to generate the final vault. The pairs in C do not lie on the polynomial. Within the final vault, the points are not known whether they belong to set G or C. At verification, only when the biometrics representation of the authenticator has substantial overlap with the enrolled user, the pairs lying on the polynomial can be identified and the key can be reconstructed. A few implementation works have been reported in [4][5][6] based on fingerprints.

A common problem in the existing solutions is that the key is changeable, but the biometrics signal is not. If the biometrics signal of an individual is compromised, all the keys generated using that biometrics signal will be compromised. Also, except Feng et al's work on iris, which in general has small variation, the other works all produce high error rate.

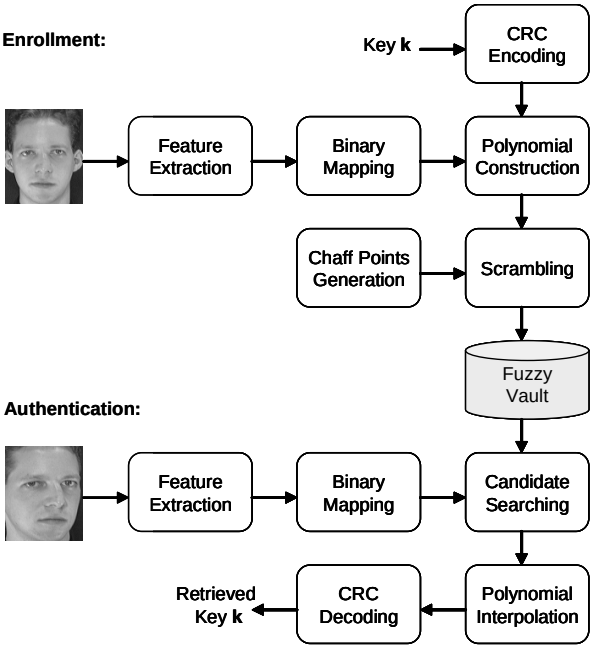

Fig. 1. General framework of proposed method

The fuzzy vault scheme offers attractive properties in terms of security (proven information-theoretic secure [8]), changeable key (generated randomly), and flexibility (working with unordered set). It is a good candidate for biometrics based cryptographic systems. In this paper, we report our implementation of fuzzy vault in a face verification problem. A two factor scheme involves user dependent random mapping is further introduced to address the changeability of biometrics signal and verification accuracy issues.

3. PROPOSED METHODS

This section presents the proposed methods for face based cryptographic key generation. Fig. 1 depicts the diagrammatic representation of the proposed solution. A set of biometrics features is first extracted from the user's face images. The extracted features are then quantized and mapped to binary representation for feature points matching. The produced binary features and the randomly generated key are bound using the fuzzy vault scheme. During authentication, the cryptographic key will be correctly retrieved if the presented authentication face features have substantial overlap with the enrolled ones. The details of the proposed methods are presented in this section.

3.1. Feature Extraction

In this paper, Principal Compoment Analysis (PCA) is adopted as the feature extractor. PCA is an unsupervised learning technique which provides an optimal, in the least mean square

1-4244-1549-7/07/$25.00

error sense, representation of the input in a lower dimensional space. In the Eigenfaces method [13], given a training set $\mathcal{Z} = \{\mathcal{Z}_i\}_{i=1}^{C}$, containing C classes with each class $\mathcal{Z}_i = \{\mathbf{z}_{ij}\}_{j=1}^{C_i}$ consisting of a number of face images $\mathbf{z}_{ij}$, a total of $N^{'} = \sum_{i=1}^{C} C_i$ images, the PCA is applied to the training set $\mathcal{Z}$ to find the $N^{'}$ eigenvectors of the covariance matrix,

$$\mathbf{S}_{cov} = \frac{1}{N'} \sum_{i=1}^{C} \sum_{j=1}^{C_i} (\mathbf{z}_{ij} - \bar{\mathbf{z}})(\mathbf{z}_{ij} - \bar{\mathbf{z}})^T \quad (1)$$

where $\bar{\mathbf{z}} = \frac{1}{N'} \sum_{i=1}^{C} \sum_{j=1}^{C_i} \mathbf{z}_{ij}$ is the average of the ensemble. The Eigenfaces are the first $N(\leq N^{'})$ eigenvectors corresponding to the largest eigenvalues, denoted as Ψ. The original image is transformed to the N-dimensional face space by a linear mapping:

$$\mathbf{y}_{ij} = \Psi^T (\mathbf{z}_{ij} - \bar{\mathbf{z}}) \quad (2)$$

where the basis vectors Ψ are orthonormal. The subsequent classification of face patterns can be performed in the transformed face space.

3.2. Binary Mapping

Unlike fingerprints, where the coordinates of the minutiae points can be used for feature matching, the extracted PCA features are a set of real numbers, and generally exact matching is impossible. One method is to perform the matching of feature points based on closeness. However, it is not clear how to define the closeness. In this paper, we propose a method to produce binary representation of face features based on 2-dimensional quantization of the distance vectors between the extracted features and pairs of random vectors. The procedure of producing binary features is as follows:

1. Extract feature vector $\mathbf{y} \in \Re^N$ from the biometrics data
2. Generate two random matrices of size $N \times M, D + 1 \leq M \leq N$, where D is the order of the polynomial for fuzzy vault construction. Apply the Gram-Schmidt method to transform them into orthornormal matrices Q_1 and Q_2.
3. Generate two random vectors $\mathbf{r}_1$ and $\mathbf{r}_2$, of length M, the elements of $\mathbf{r}_1$ and $\mathbf{r}_2$ are uniformly distributed in [0 τ], where τ is a preset value.
4. Compute $R_{1i} = Q_{1i} \cdot \mathbf{r}_{1i}$ and $R_{2i} = Q_{2i} \cdot \mathbf{r}_{2i}, i = 1.....M$, where the subscript i denotes the i^{th} column vector in (Q_1, Q_2) and i^{th} element in $(\mathbf{r}_1, \mathbf{r}_2)$.
5. Compute the Euclidean distance between $\mathbf{y}$ and each column vectors in R_1 and R_2, $\mathbf{d}_{1i} = \|\mathbf{y} - R_{1i}\|^2$ and $\mathbf{d}_{2i} = \|\mathbf{y} - R_{2i}\|^2$.
6. Quantize $\mathbf{d}_{1i}$ and $\mathbf{d}_{2i}$ into 256 steps and map to binary bit strings $\mathbf{b}_{1i}$ and $\mathbf{b}_{2i}$;
7. The final binary features are generated by concatenating the corresponding bits in $\mathbf{b}_{1i}$ and $\mathbf{b}_{2i}$, i.e., $\mathbf{b}_i = [\mathbf{b}_{1i}|\mathbf{b}_{2i}], i = 1.....M$.

By using the proposed method, the N-dimensional face features are mapped to M 16-bit binary features. The usage of two distance vectors allows for projecting the binary features onto a square tessellation of a 2-D image plane, where $\mathbf{b}_{1i}$ and $\mathbf{b}_{2i}$ correspond to the coordinate along x and y axes respectively. This will improve the accuracy of feature points matching since the binary feature $\mathbf{b}_i$ will match if and only both $\mathbf{b}_{1i}$ and $\mathbf{b}_{2i}$ match. Due to the randomness of R_1 and R_2, the projection of a feature $\mathbf{y}$ onto the two axes are independent. The orthogonization procedure in step 2 produces uncorrelated binary strings along each direction. Step 3 and 4 produces orthogonal vectors of different norm. This will facilitate the quantization and also spread the binary features over the whole plane, therefore increase the difficulty for an adversary to conduct brute-force attack.

3.3. Fuzzy Vault Encoding

Juels and Sudan [8] proposed to use Reed-Solomon (RS) codes for error correction. However, it is not clear how to perform RS decoding since the encoding algorithms of fuzzy vault is not the same as RS coding, and therefore RS decoding can not be applied to decode the vault [14]. In this paper, a similar scheme as proposed in [5] is adopted for fuzzy vault encoding and decoding. A 128-bit random bit string $\mathbf{k}$ is first generated using a random number generator. The bit string $\mathbf{k}$ is the cryptographic key that needs to be protected and linked with the biometrics signal. To ensure correct recovery of the key from the fuzzy vault, $\mathbf{k}$ is encoded using Cyclic Redundancy Check (CRC). The CRC-16 polynomial, $g(x) = x^{16} + x^{15} + x^2 + 1$, is used for CRC generation. By appending the 16-bit CRC to the 128-bit $\mathbf{k}$, a new 144-bit code $\mathbf{k}_{crc}$ is generated. This $\mathbf{k}_{crc}$ is used for construction of the fuzzy vault.

A 8-order polynomial, $f(x) = c_8x^8 + c_7x^7 + ... + c_1x + c_0$, is selected for binding of $\mathbf{k}_{crc}$ and the binary biometrics features $\mathbf{b}_i, i = 1...M$. The 144-bit $\mathbf{k}_{crc}$ is truncated to 9 non-overlapping 16-bit segments, and each of them are mapped to the coefficients $c_0 - c_8$. The order of the mapping should be consistent for encoding and decoding of the vault. The polynomial $f(x)$ is then evaluated on each of the feature points $\mathbf{x}_i$, where $\mathbf{x}_i$ is an integer number corresponds to the binary feature $\mathbf{b}_i$. The generated pairs $\{(\mathbf{x}_i, f(\mathbf{x}_i)), i = 1...M\}$ are termed the genuine set G. Then we generate the chaff points set $C = \{(a_j, b_j), j = 1...N_c\}$, where $N_c \gg M, a_j \neq \mathbf{x}_i$, and each pair does not lie on the polynomial, i.e., $b_j \neq f(a_j)$. The final vault is constructed by taking the union of the two set, $G \cup C$, and pass through a scrambler so that it is not clear which are the feature points and which are the chaff points, $\{V = (\mu_k, \nu_k), k = 1...M + N_c\}$.

1-4244-1549-7/07/$25.00

3.4. Fuzzy Vault Decoding

The decoding of the fuzzy vault is based on polynomial reconstruction. An authenticator presents his binary biometrics features $\mathbf{b}_i^*$, and search for the matchings in the fuzzy vault *V*. To tolerate errors introduced due to the noisy nature of biometrics signal, a windowing process is applied. $\mathbf{b}_i^*$ is divided into two 8-bit trunks corresponding to the x and y direction of the 2-D image plane. All the fuzzy vault points that falls into the $\pm w$ window in the image plane are treated as candidate points. All the candidate points are identified and together with their pair values in the vault form a set *S*. Let *K* denotes the number of pairs in *S*, for the reconstruct of a polynomial of degree *D*, all possible combinations of $D+1$ points are identified, with a total number of $\binom{K}{D+1}$ combinations. Each of the possible combinations is used to recover the polynomial using Lagrange interpolating technique. For example, given an identified combination $\{(\mu_1,\nu_1),(\mu_2,\nu_2),...,(\mu_{D+1},\nu_{D+1})\}$, the polynomial can be reconstructed as: $f(x)=\sum_{i=1}^{D+1} f_i(x)$, where $f_i(x)=\nu_i\prod_{j=1,j\neq i}^{D+1}\frac{x-\mu_j}{\mu_i-\mu_j}$ [15]. The coefficients in the generated polynomial is mapped back and concatenated in the same order as encoding to generate a 144-bit code $\mathbf{k}_{crc}^*$. To check the correctness of the decoding, $\mathbf{k}_{crc}^*$ is divided by the CRC polynomial $g(x)$. If the remainder is zero, then with high probability $(1-2^{-16})$ no error occurs [5]. The cryptographic key $\mathbf{k}$ can be retrieved by taking the first 128 bits of $\mathbf{k}_{crc}^*$.

3.5. User-independent *vs* User-dependent

The proposed method for cryptographic key generation can be implemented in two different scenarios: user-independent and user-dependent. In the user-independent scenario, all the users use the same sets of random matrices (R_1,R_2), while in the user-dependent scenario, each user is associated with a distinct sets of (R_1,R_2). Due to the distance vectors are used and quantized as the binary features, the spatial closeness of features from genuine users can be approximately preserved. For the user-independent scenario, the discriminant characteristics of the binary features between different users depends on the separability of the extracted face features in terms of spatial distance.

For the user-dependent scenario, due to the randomness of (R_1,R_2) for computing the distance vectors, the probability of false matching will be very small. The evaluation can be performed based on hypothesis testing: $\mathbf{H}_0$: the authenticator is a genuine user; $\mathbf{H}_1$: the authenticator is an imposter. The false accept rate (FAR) corresponds to $P(\mathbf{H}_0|\mathbf{H}_1)$ and false reject rate (FRR) corresponds to $P(\mathbf{H}_1|\mathbf{H}_0)$. FAR and FRR are related functions of system parameters (*M* and *w* in the proposed system). Assume the genuine and imposter's feature points are randomly projected onto the 2-D plane, and there is no overlap between the searching window of an imposter. For the fuzzy vault with polynomial of degree $D=8$, the probability of having $k\geq 9$ genuine points fall into the searching window (size $(2w+1)^2$) of an imposter can be computed as $P(\mathbf{H}_0|\mathbf{H}_1)=\sum_{k=9}^{M}p_k$, where $p_k=\binom{M}{k}p^k(1-p)^{M-k}$, and $p=\frac{k(2w+1)^2}{256^2}$. For example, if $M=20, w=2$, then $P(\mathbf{H}_0|\mathbf{H}_1)=1.08\times10^{-17}\approx 0$. Therefore, by setting system parameters such that FRR=0, zero error rate can be achieved. This also explains the changeability of biometrics signal since even the same biometrics features are presented, if (R_1,R_2) are different, correct matching can not be obtained. Fig. 2 demonstrates the fuzzy vault matching in the projected 2-D image plane. It can be observed that the genuine and imposter points are very well separated in the user-dependent scenario.

4. EXPERIMENTAL RESULTS

To evaluate the performance of proposed methods, we conducted our experiments on a well known public face databases ORL [16]. The ORL database contains 400 face images from 40 subjects with 10 images each. For some subjects, the images were taken at different times, varying the lighting, facial expressions, and facial details. All the images were taken against a dark homogeneous background with the subjects in an upright, frontal position (with tolerance for some side movement).

In this paper, The evaluation is based on false accept rate (FAR), false reject rate (FRR), and equal error rate (ERR), which is defined as the operating points where FAR and FRR are equal. The first 5 images of each subject is used as training set as well as the gallery set, and the rest as testing set. All the images are transformed to the PCA domain and the first 20 coefficients are used as face features. The mean of the distance vectors of the gallery set of each person is used for fuzzy vault encoding while the other images for decoding. An empirical value of $\tau=200$ is selected for generation of norm spreading vectors $(\mathbf{r}_1,\mathbf{r}_2)$. The experiments are performed on $M=9-20$ number of binary features, with searching window size $w=1-5$. To minimize the effect of randomness, all the experiments were performed 5 times and the average of the results are reported.

4.1. User-independent

In the user-independent scenario, all the users use a global set of (R_1,R_2). Table 1 details the obtained EER with respect to different number of binary features *M* and window size *w*. Fig. 3 depicts the receiver operating curve (ROC) as a function of *M* and *w*. It can be observed that as the window size increases, FAR increases and FRR decreases. This is because the increase of *w* will introduce imposter points into the matching window. The same behavior presents as the number of binary features *M* increase. The selected polynomial require 9 matched points. If the number of available points increase, the possibility of matching will increase.

1-4244-1549-7/07/$25.00

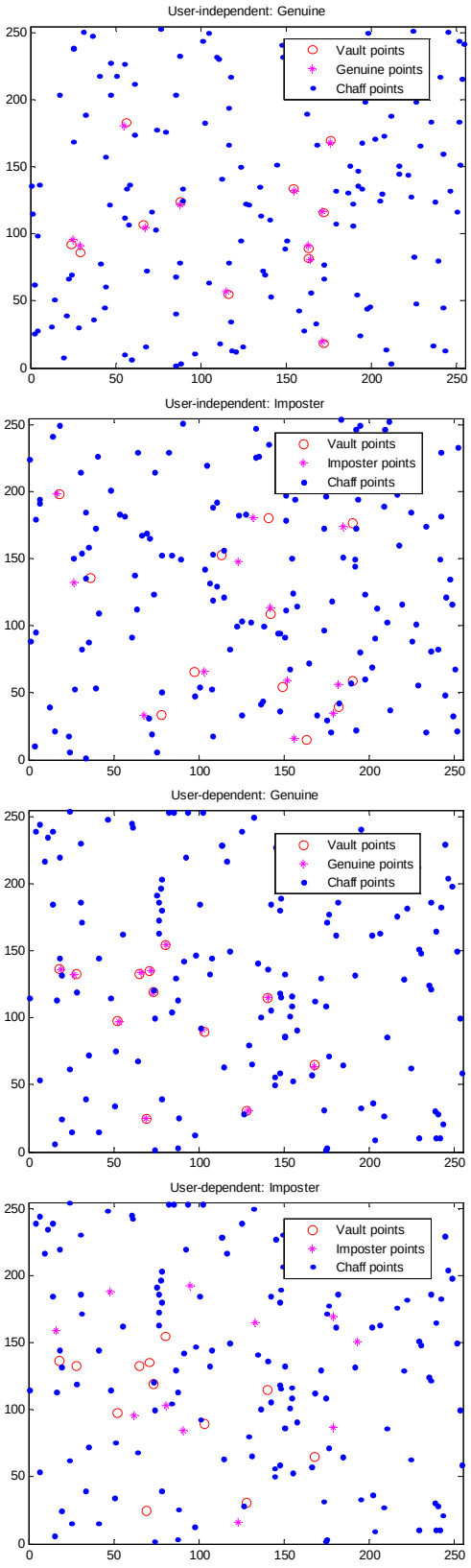

Fig. 2. Demonstration of fuzzy vault matching

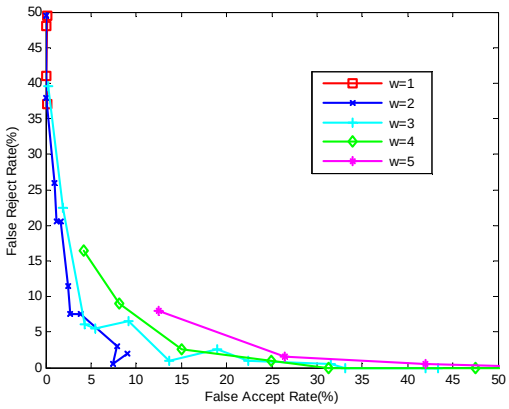

Fig. 3. ROC curve as a function of M and w

		w=				
		1	2	3	4	5
M=	9	49	38.75	19.87	10.33	10.26
	10	47	24.8	12.18	8.58	13.96
	11	41.75	19.04	5.15	8.78	2.13
	12	39.75	13.47	5.5	12.97	29.51
	13	38.26	10.87	7.83	15.62	32.47
	14	35.76	11.06	7.3	23.79	36.11
	15	33.5	6.99	10.72	28.44	38.08
	16	30	5.08	11.71	32.14	43.61
	17	24.01	5.65	16.01	37.13	44.31
	18	24.81	5.42	16.55	36.06	45.94
	19	20.52	3.94	21.67	40.32	46.63
	20	18.58	5.53	20.97	43.28	48.28

Table 1. EER (%) obtained in the user-independent scenario with different M and w.

In our experiments, the best results obtained in terms of EER is 3.94%, with FAR=7.38% and FRR=0.5%, at $M = 19$ and $w = 2$. For comparison purpose, we also performed experiments using the same 20 PCA features in a verification scenario. Euclidean distance is used as the metric, and the classification is based on nearest neighbors. The experiments produces an EER of 6.25%. It is clear that the proposed method produces promising results.

4.2. User-dependent

In the user-dependent scenario, each user is associated with a specific set of (R_1, R_2). These can be linked with a password or stored in a token. Table 2 details the obtained EER with respect to different number of binary features M and window size w. By properly setting M and w, the proposed two-factor scheme is capable of producing zero EER.

There are two scenarios that need to be considered for a two-factor scheme: stolen password (token), and stolen bio-

1-4244-1549-7/07/$25.00

		w=				
		1	2	3	4	5
M=	9	48.75	34.75	20.25	10	3.75
	10	46.75	30.75	12.75	6	2
	11	44.75	23.25	8.25	3.5	1.75
	12	43.25	19.25	7.75	2.25	0
	13	40.25	14	5.5	2.25	0.25
	14	37.25	12.5	4	0.25	0
	15	35.25	11.25	2.5	0.75	0
	16	33.25	9.25	2	0.5	0
	17	30.25	9.25	2	0	0
	18	29.75	7.5	1.25	0	0
	19	30	6.75	0.75	0	0
	20	25.5	5	0.5	0	0

Table 2. EER (%) obtained in the user-dependent scenario with different *M* and *w*.

metrics. The stolen password (token) scenario is essentially the same as the user-independent case where the same set of (R_1, R_2) are used. In the stolen biometrics scenario, due to different sets of (R_1, R_2) are used, the mapped points in the 2-D plane do not match the genuine points. Therefore even an adversary steals a user's biometrics, without presentation of the correct (R_1, R_2), verification will be failed. We performed experiments in the stolen biometrics scenario, where different (R_1, R_2) are applied to biometrics signals of the same user. In our experiments, FAR=0 is produced in all *M* and *w* settings. This also accounts for the changeability of biometrics since by changing *M* and *w*, the old biometrics representation can not be used for successful authentication.

5. CONCLUSION

This paper introduced a systematic framework for addressing the challenging problem of generating changeable cryptographic key from noisy face biometrics. The proposed method utilize a previously introduced method, *fuzzy vault*, for secure binding of biometrics features with randomly generated cryptographic keys. To tolerate the variations of biometrics signals, a method based on 2-D quantization of distance vectors is proposed. Experimentation shows that the proposed solution achieves promising results. Further, we also present a two-factor scheme, where user-dependent external input is integrated with biometrics features. This scheme provides changeability for biometrics signals, and produces zero EER.

In this paper, we focus on face based cryptographic key generation problem. However, the proposed solutions are general and can also be applied to other biometrics molalities. A major problem with the current fuzzy vault based scheme is the computational complexity. In the future, we are going to elaborate the proposed methods by introducing error correction techniques, and study new methods for fast and secure binding of biometrics with cryptographic keys.

6. REFERENCES

[1] NIST, Advanced Encryption Standard(AES), 2001 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

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

[3] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition", IEEE Trans. on Circ. and Sys. for Video Tech. vol. 14, no. 1, pp. 4-20,Jan. 2004

[4] R. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smart card based fingerprint aithentication", Proc. of ACM SIGMM Workshop on Biometrics Methods and Applications, pp. 45-52, 2003

[5] U. Uludag, S. Pankanti, and A. Jain, "Fuzzy vault for fingerprints", Proc. of Int. Conf. on Audio and Video based Biometric Person Auth., pp. 310-319, 2005

[6] S. Yang and I. Verbauwhede, "Secure fuzzy vault based fingerprint verification system," Proc. Asilomar Conf. on Sig., Sys., and Comp., Vol. 1, pp. 577-581, Nov. 2004

[7] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometric effectively", IEEE Trans. on Computers, vol. 55, no. 9, pp. 1081-1088, 2006

[8] A. Juels, and M. Sudan, "A fuzzy vault scheme", Proc. of IEEE Int. Symp. on Info. Theory, pp. 408, 2002

[9] A. Bodo, Method for producing a digital signature with aid of a biometric feature, German Patent DE 42 43 908 A1, 1994

[10] Y. J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation", Proc. of IEEE Int. conf. on Multimedia and Expo, pp. 2203-2206, 2004

[11] A. Juels, and M. Wattenberg, "A fuzzy commitment scheme", Proc. of sixth ACM Conf. on Computer and Communication Security, pp. 28-36, 1999

[12] A. Kholmatov, B. Yanikoglu, E. Savas, and A. Levi, "Secret sharing using biometric traits", Proc. of SPIE, vol. 6202, pp. 62020W-1-9, 2006

[13] M. Turk, A. Pentland, "EigenFaces for recognition", Journal of Cognitive Neuroscience 13(1) (1991) 71-86

[14] Q. Li, Z. Liu, and X. Niu, "Analysis and problems on fuzzy vault scheme", Proc. of Int. conf. on Intell. Info. Hiding and Multimedia Sig. Processing, pp. 244-250, 2006

[15] Wolfram MathWorld, Lagrange Interpolating Polynomial, http://mathworld.wolfram.com/LagrangeInterpolatingPolynomial.html.

[16] ATT Laboratories Cambridge, ORL face databse, www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html.

1-4244-1549-7/07/$25.00