Hindawi Publishing Corporation
ISRN Machine Vision
Volume 2014, Article ID 161932, 13 pages
http://dx.doi.org/10.1155/2014/161932

*Research Article*

# A New Scheme for the Polynomial Based Biometric Cryptosystems

**Amioy Kumar, M. Hanmandlu, and Hari M. Gupta**

*Biometrics Research Laboratory, Department of Electrical Engineering, Indian Institute of Technology Delhi, Hauz Khas, New Delhi 110 016, India*

Correspondence should be addressed to Amioy Kumar; amioy.iitd@gmail.com

Received 29 September 2013; Accepted 5 December 2013; Published 22 April 2014

Academic Editors: M. Leo and N. A. Schmid



This paper presents a new scheme for the fuzzy vault based biometric cryptosystems which explore the feasibility of a polynomial based vault for the biometric traits like iris, palm, vein, and so forth. Gabor filter is used for the feature extraction from the biometric data and the extracted feature points are transformed into Eigen spaces using Karhunen Loeve (K-L) transform. A polynomial obtained from the secret key is used to generate projections from the transformed features and the randomly generated points, known as *chaff points*. The points and their corresponding projections form the ordered pairs. The union of the ordered pairs from the features and the chaff points creates a fuzzy vault. At the time of decoding, matching scores are computed by comparing the stored and the claimed biometric traits, which are further tested against a predefined threshold. The number of matched scores should be greater than a tolerance value for the successful decoding of the vault. The threshold and the tolerance value are learned from the transformed features at the encoding stage and chosen according to the tradeoff in the error rates. The proposed scheme is tested on a variety of biometric databases and error rates obtained from the experimental results confirm the utility of the new scheme.

## 1. Introduction

Intrusions in the secret data protection arena pose potential threat to the information security. In the recent trends of the data protection, biometrics based cryptosystems are emerging as promising technologies. Biometric cryptosystems can be broadly divided into two main schemes: (a) *Key binding mode*, in which the secret key is integrated with the biometric template. In this mechanism, both the biometric template and the key are so locked that it is very difficult to retrieve any one without the information of other [1–4]. (b) *Key generation mode*, in which the biometric template generates the keys used in any cryptographic algorithm for the encryption and decryption of secret messages [5–8]. Both the approaches are secure and computationally very difficult for the intruder to attack. However, these approaches pose implementation problems as it requires the encryption key to be exactly same as the decryption one. But the biometric data acquired at different times is substantially different, due to the intraclass variations, necessitating a different key every time.

The implementation of key binding mode is greatly affected by the cryptographic construct called fuzzy vault, investigated by Juels and Sudan [9]. This fuzzy vault can tolerate the intraclass variability in the biometric data, which has inspired several researchers [1–4] to pursue the biometrics based fuzzy vaults. This paper proposes another attempt on using fuzzy vault scheme in key binding mode by presenting a new scheme which exploits textural features from biometric traits.

*1.1. The Prior Work.* Both the key binding mode [1–4, 10] and the key generation mode [5–8, 11] of biometric cryptosystem have been addressed in the literature. Moreover, prevention of the attacks on the biometric templates is also addressed by using the nonrevocable biometrics [12–14] and BioHashing [11, 15–18]. One widely accepted solution to the intrusion of the stored biometric templates is the reissuance of biometric features.

The key generating mode of the biometric cryptosystem is of particular interest in [6–8, 11, 19]. Hao et al. [6] select

iris for generating the cryptographic keys with the help of the hybrid Reed & Solomon and Hadamard error correcting codes. Sauter et al. [7] resort to the key generation using the fingerprints and their work has resulted in the product, *Bioscrypt*. Instead of generating a key directly from biometrics, they have devised a method of biometric locking using the phase product. A fuzzy extractor based approach is suggested by Dodis et al. [8] to generate a strong cryptographic key from the noisy biometric data. This scheme is modified by Boyen [19] by generating multiple keys before hashing.

The basic idea of a key binding was borrowed from the work of Juels and Sudan [9] which was an extension of the work in [20]. They introduce the polynomial construction to hide the secret key with integration of an unordered set and modify the fuzzy vault scheme of Davida at el. [13] by invoking Reed and Solomon error correcting code [21]. However, Uludag et al. [1] were among the first to investigate the fuzzy vault using the fingerprint biometric as an unordered set. The difficulties associated with the minutiae point alignment are significantly reduced in [4] with the *helper data* during the minutiae point extraction. A modified fuzzy vault is suggested in [22] where the secret key and the biometric features are hidden in separate grids with chaff points added to make the grids fuzzy. The same scheme makes its way in a palmprint based vault [23].

*1.2. The Motivations.* Note that fingerprint has been utilized as a biometric trait [1–4] in most of the published work on polynomial based fuzzy vault. In the context of fingerprint authentication, minutiae points are widely accepted as the most significant features [4]. The minutiae points are the specific locations in a finger and can be considered as ordered triplet $(x, y, \theta)$ [4]. But since the points are associated with their locations and saved accordingly, they become an unordered set which can be shuffled without losing its significance and can be matched with original set in any order. Despite the current popularity of other biometric traits like palmprint, iris, and hand veins, there are less attempts to use them in the polynomial based fuzzy vault. In this direction, iris [24], palmprint [25], and handwritten signature [26] based cryptosystems merit a mention. Here, the work in [24] made use of clustering method to make iris features unordered while the other two cryptosystems operate on key generation mode. The reason for lack of interest could be the orderliness of the features extracted from these traits. The orderliness of these features implies that any change in their order will result in a new set of features that can affect the authentication process.

*1.3. The Proposed Work.* This paper devises a new scheme for the polynomial based fuzzy vault, in the key binding mode, by employing the textural features generated using Gabor filters of the biometric traits [27]. In the proposed approach, Karhunen Loeve (K-L) transform [28] to transform the features into the Eigenspace through the transformation matrix (Eigenvector matrix). The projection of the transformed features is taken on the polynomial and chaff points are added to form the fuzzy vault. The original and the transformed features are discarded after creating the vault. However, the transformation matrix is stored along with the vault to be used during the decoding process. Essentially, a query feature vector is transformed using the stored transformation matrix. Each point of the transformed query feature vector is subtracted from all the stored vault points, and the differences are matched against a cutoff threshold. If the difference is less than this threshold, the corresponding biometric feature point is supposed to be the original feature vector. However, only $N + 1$ features are required to reconstruct a polynomial of degree $N$ and an original feature set may have more points than $N$. Thus, total count of such feature points should be greater than a tolerance value for the claimed identity to be true. The cutoff threshold and tolerance value are learned from the transformed features (before being discarded) at the time of encoding. The reconstruction of the polynomial of any query takes place only when these two thresholds are validated. These values can also be compared with the decision thresholds in the traditional biometric authentication, chosen according to the tradeoff between the error rates (false acceptance/rejection).

The usage of the Gabor filter based features in the vault allows this scheme to be generalized for many biometric traits. The proposed scheme is tested on variety of publicly available databases, that is, FVC 2004 DB2, Hong Kong PolyU V2, and CASIA V1 of fingerprint, palmprint, and iris, respectively, including the hand vein database of IIT Delhi with the textural features extracted using Gabor filters**.** The experimental results show that the presented approach operates on lower error rates and can be acceptable for any security applications. It is remarked that no existing biometric cryptosystem is tested on such a variety of publicly available databases. The block diagram of the complete approach is shown in Figure 1.

The rest of the paper is organized as follows. Section 2 presents an overview on implementation of the earlier proposed fuzzy vault and the modifications done in our scheme. Section 3 details the proposed scheme of the fuzzy vault. The experimental results are presented in Section 4, and some security-related issues are discussed in Section 5. Finally, a summary of the overall work is outlined in Section 6.

## 2. An Overview on Fuzzy Vault

*2.1. The Fuzzy Vault.* The fuzzy vault introduced by Juels and Sudan [9] contains a secret key integrated with an unordered set using polynomial projections. The key can be accessed through the polynomial reconstruction using another unordered set, if the set is much similar to the original one. The fuzzy vault is used as biometric cryptosystem in [2] with the minutiae points of the fingerprint as an unordered set. In this work, the polynomial coefficients are computed from the secret key and the projections of the minutiae points are taken on this polynomial. The added chaff points are such that they do not lie on the generated polynomial. Let secret key $S$ (e.g., cryptographic key) be hidden using a biometric feature set $T = \{t_1, t_2 \cdots t_r\}$ of length $r$. Error correcting bits are added to the secret key $S$ to form $S1$ to tolerate the errors created at the time of decoding. The coefficients of the polynomial are generated using $S1$. Let

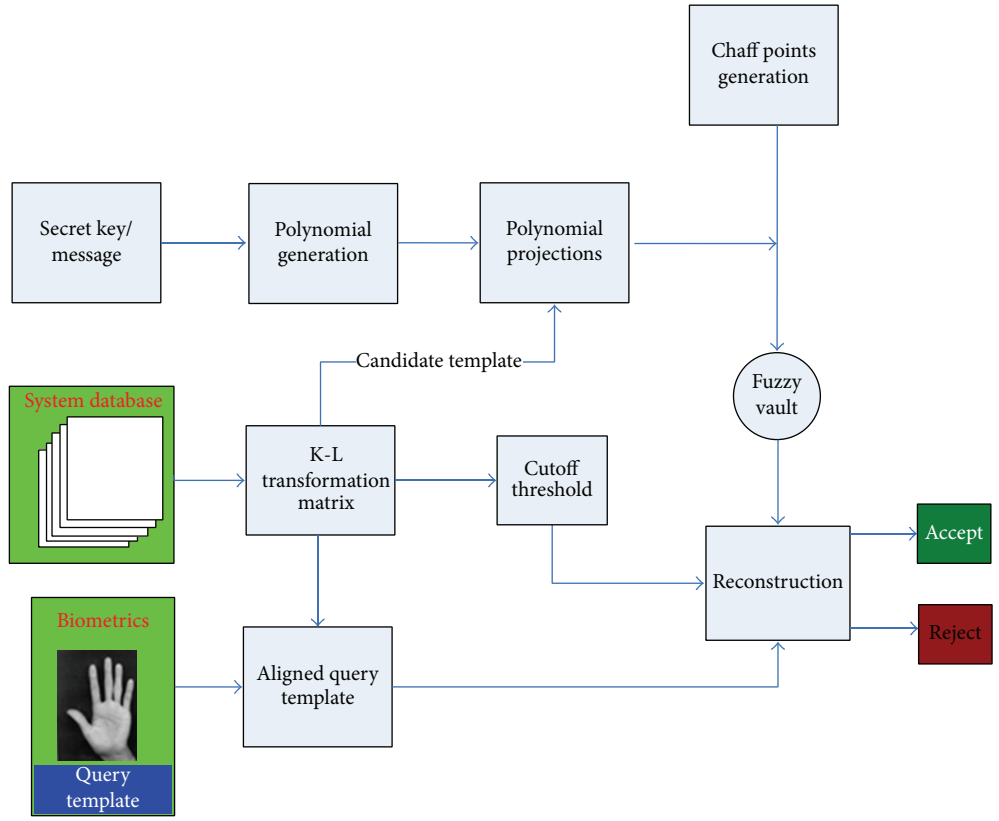



Figure 1: Block diagram of the complete system.

$P(x) = a_0 + a_1 x + \cdots + a_{(n-1)} x^{N-1}$ be the polynomial of degree $N - 1$ formed from $S1$. The projection of each element of $T$ on the polynomial $P$ together with element itself forms a couplet $(t_k, P(t_k))$. The chaff couplet $(u_i, v_i)$ is generated such that $P(u_i) \neq v_i$. The union of feature couplet $(t_k, P(t_k))$ and chaff couplet $(u_i, v_i)$ creates the vault $\mathbf{V}$. The secret key $S$ and the feature $T$ are thus integrated and bind in the fuzzy vault.

At the unlocking step, the user provides a query template denoted by $T' = \{t'_1, t'_2 \cdots t'_r\}$ of "$r$" elements. If $T'$ overlaps substantially with $T$, the user can retrieve many original points from $\mathbf{V}$ that lie on the polynomial. These overlaps help reconstruct the polynomial coefficients and thereby the secret key $S$. If the number of discrepancies between $T$ and $T'$ is less than $(r - n)$, $n$ overlaps are needed to interpolate the polynomial. Error checking is one way to check whether the set of overlaps chosen is appropriate to decode the vault. On the other hand, if $T$ and $T'$ do not have a sufficient overlap, $P$ cannot be reconstructed; hence the authentication fails. The vault is called *fuzzy* because the added chaff points to the original biometric features make them so vague that it cannot be separated without the presence of original features.

The crucial parameters in the vault implementation are $R$, $N$, and $C$, where $R$ is the number of features used in the vault encoding, $N$ is the degree of the polynomial chosen according to the length of the secret message in the vault, and $C$ is the number of chaff points added to the vault for concealing the original data points from an attacker.

*2.2. Modifications in the Earlier Approach.* The new scheme for fuzzy vault, presented in this paper, has the following main differences from the earlier schemes [2–4, 29].

(1) The textural features extracted using Gabor filters are attributed as one of the most significant features in palmprint [27], iris [30], and even fingerprint [31]. Note that the use of these features is made for the first time in the polynomial based fuzzy vault. To separate out the original points from the chaff points, a cutoff threshold and a tolerance value are learned empirically at the encoding phase of the vault. A novel scheme for the generation of the polynomial coefficients from the secret key is also developed.

(2) One parity check bit is added to each binary string of the secret message/key. The binary strings are formed from the secret key by splitting the key into $N$ parts, where $N$ is the number of coefficients of the polynomial. The reconstruction of the polynomial is successful only if the parity check bit is unaltered. Otherwise, this gives rise to the false acceptance/rejection error.

(3) At the learning phase, the biometric features are employed to construct the transformation matrix of Eigenvectors. The original feature vector is then transformed and the transformed feature vector is used for the polynomial projection. The cutoff threshold is also learned at this phase using the transformed feature

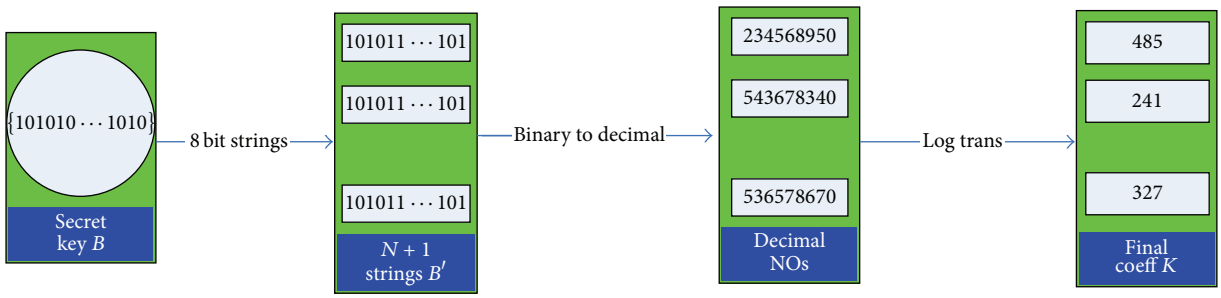



Figure 2: Block diagram for generating polynomial coefficients.

vector. After the vault is generated, both the original and transformed feature vectors are discarded for the security reasons. However, the transformation matrix (i.e., Eigen vector matrix) is retained for the assessment of the query features toward the access to the authentication system.

## 3. The Proposed Scheme for the Fuzzy Vault

*3.1. Generation of the Polynomial Coefficients.* A secret key $S$ of lengths $B$ bits is randomly generated. For a polynomial of degree $N$, a total of $N + 1$ number of coefficients should be generated from the random bits $B$. So, $B$ is divided into $N + 1$ binary strings denoted as $B'$. With each $B'$, a cyclic redundancy check (CRC) bit is added to every string. At the authentication stage, these bits are checked after the reconstruction of the polynomial coefficients and any discrepancy in these bits is declared as an unsuccessful attempt to the access of the vault.

Each of bit strings $B'$ is converted to a decimal number and then the logarithmic transformation is applied on the decimal numbers to bring them into the lower range of values that become the polynomial coefficients $K$. The block diagram in Figure 2 shows the stages in the generation of the polynomial coefficients. We have 384 randomly generated bits $B$, which are split into $B' = 8$ strings of equal length. One bit of CRC is added to each $B'$ and converted into its decimal equivalent, which is subjected to the logarithmic transformation (base 2) to yield the coefficients of the polynomial.

In the proposed scheme, a polynomial of degree 7 is chosen to hide the secret key of 384 bits. Any secret key of more than this length can be hidden by choosing a polynomial of higher degree. The method in [4] uses an 8 degree polynomial to hide a secret of 128 bits.

*3.2. Significant Features for Encoding.* K-L transform, also known as PCA (principal component analysis), is used to extract the significant features [28]. In the proposed scheme, the transformation matrix arising out of the K-L transform facilitates the determination of the subspace of the original feature vector for encoding the vault. The same transformation matrix is applied on the query feature vector to convert it into the same subspace for aligning (matching) with the fuzzy vault.

Let $\{S\}_{N1\times 1}$ denote the feature vector of size $N1$ extracted from the biometric trait. The covariance matrix $\{M\}_{N1\times N1}$ is constructed from $S$. The Eigenvector matrix $\{V\}_{N1\times N1}$ corresponding to the Eigenvalues $\{\lambda\}_{N1\times 1}$ of $M$ spans the feature subspace. The extracted features sometime contain redundant data which can increase the error rates (FAR/FRR) in the vault implementation. Hence $S$ has to be reduced to the chosen dimension $k$ and $\{\delta\}_{k\times 1}$ can be made up of Eigen vectors corresponding to the dominant Eigen values $\{\lambda\}_{k\times 1}$ by multiplying the transformation matrix $\{V\}_{k\times N1}$ as follows:

$$\{\delta\}_{k\times 1} = \{V\}_{k\times N1} \times \{S\}_{N1\times 1}. \quad (1)$$

The transformed feature vector is used to learn the cutoff threshold ($\alpha$) and the tolerance value ($\beta$). The cutoff threshold is taken as the maximum of the pointwise differences between the training feature vectors. The tolerance value is determined from the ROC curve for each modality. The cutoff threshold and tolerance value are fine-tuned as per the specified error rates to be achieved.

*3.3. Encoding of the Vault.* Let the transformed feature vector $\{\delta\}_{k\times 1}$ be represented by $\{\theta_1, \theta_2 \cdots \theta_k\}^T$, whose projections on the polynomial $P$ of degree $N$ form the projection set $P_r = \{P(\theta_1), P(\theta_2) \cdots P(\theta_k)\}^T$. Next, $N + 1$ coefficients of $P$ computed using the secret key (detailed in Section 4.1) are saved as $K = \{C_0, C_1, C_2 \cdots C_N\}$. The elements of the projection set are obtained as

$$P(X) = C_N X^N + C_{N-1} X^{N-1} + \cdots + C_0. \quad (2)$$

The ordered pairs $\{\theta_i, P(\theta_i)\}$; $i = 1, 2, 3, \ldots, k$, are made up of point $\theta_i$ and its corresponding projection $P(\theta_i)$.

The next task is to generate the chaff points that do not satisfy $P$. In the proposed scheme, the random numbers are generated by fitting a U-distribution [32] having the mean and variance of the feature point. Any number of chaff points can be generated using this distribution corresponding to each data point $\delta_i; i = 1, 2, 3, \ldots, k$, and the generated random numbers do not coincide with any of the original $k$ features. For example, considering $\delta_i$ as mean and $[\delta_{i+1} - \delta_i]$ as variance, we can generate 10 random numbers for each data point $\delta_i$ resulting in 900 chaff points corresponding to 90 transformed feature points.

Let the chaff points $\{\mu_{i1}, \mu_{i2}, \ldots, \mu_{ig}\}$, $g$, be the random numbers for a feature point $\theta_i$. The ordered pairs $(\mu_{it}, \eta_{it})$ arise

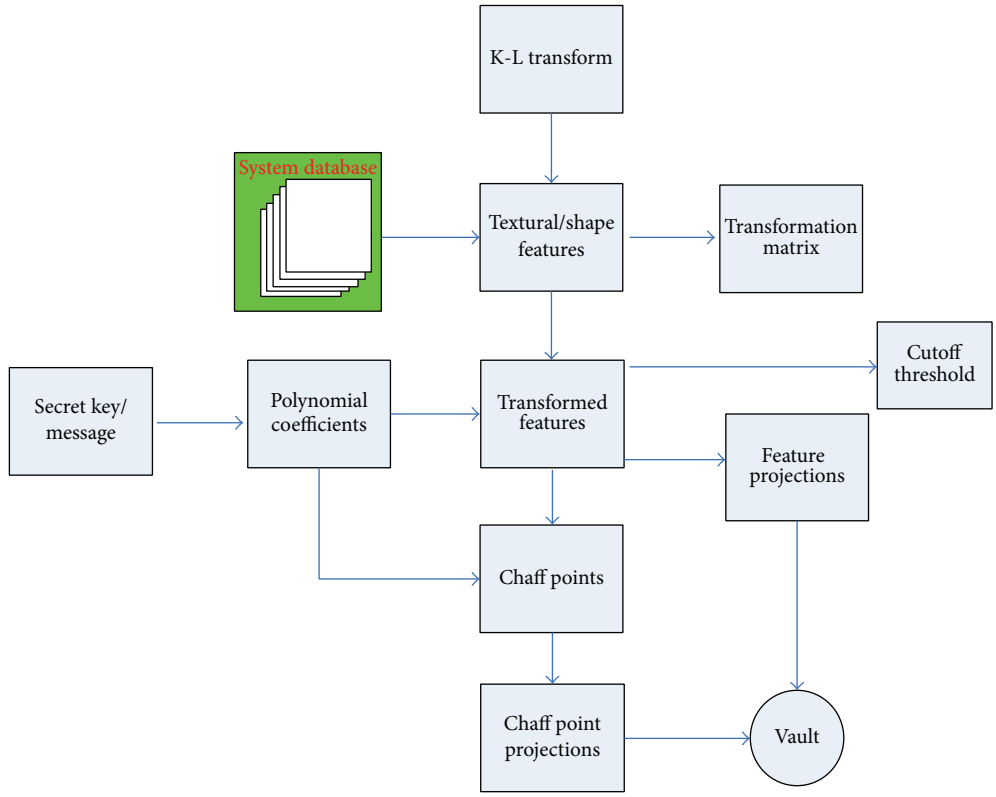



Figure 3: Encoding of the vault.

from $\mu_{it}$ such that $P(\mu_{it}) \neq \eta_{it}$. The union of the two ordered pairs $\{\theta_i, P(\theta_i)\}$ and $\{\mu_{it}, \eta_{it}\}$ for all $\theta_i$'s creates the fuzzy vault, $V$, given by

$$V = \{\theta_{i+k}, P(\theta_{i+k})\} \cup \{\mu_{it}, \eta_{it}\}. \quad (3)$$

As mentioned above, the original feature vector $\{S\}_{N1\times 1}$ and the transformed feature vector $\{\delta\}_{k\times 1}$ are removed from the database. The transformation matrix $\{V\}_{k\times N1}$, the cutoff threshold ($\alpha$), tolerance value ($\beta$), and the vault $V$ are stored for decoding. The block diagram in Figure 3 shows the modules required in encoding the fuzzy vault.

*3.4. Decoding of the Vault.* The decoding of the vault involves alignment of a query template with the stored one. This alignment of query template helps in separating the chaff points from the stored template points in the vault. In the fingerprint based fuzzy vault in [4] the minutiae features are aligned using an adaptive bounding box, which counters the distortions in the minutiae features more effectively than the approach in [2]. The approach in [4] resorts to a threshold to separate the original minutiae points from the chaff points. The basic idea is to cash in on a parameter to differentiate between the genuine and the imposter templates. In the proposed scheme, the successful decoding of the vault depends upon two parameters: the cutoff threshold ($\alpha$), learned from the transformed features $\{\delta\}_{k\times 1}$, and the tolerance value ($\beta$) which is fixed according to the tradeoff in the error rates (FAR/FRR).

The query feature vector $q = \{q_1, q_2, q_3 \cdots q_{N1}\}$ undergoes the K-L transformation $\{V_k^T\}_{k\times N1}$, to yield the transformed query feature vector $Q = \{Q_1 Q_2 \cdots Q_k\}$ of length $k$ at the encoding. Let the ordered pairs of the vault $V$ be denoted as $\{\mu, \eta\}$. Subtraction of $Q_k$ from all the abscissas of the ordered pairs in $V$ provides $(g + 1)k$ differences stored in an array $A$ as the matching score. The scores below the cutoff threshold $\alpha$ is assumed to be from original feature points, otherwise from chaff points. The ordered pairs corresponding to these scores are separated out from the vault $V$. Let $H$ of the set of ordered pairs be separated from the vault $V$. To reconstruct the polynomial coefficients $K = \{C_0, C_1, C_2 \cdots C_N\}$ only $N+1$ original (genuine) ordered pairs are needed. If $H < N + 1$ then it results in the authentication failure. If $H \geq N + 1$ the polynomial can be successfully reconstructed. However, $H$ may also exceed $N + 1$ due to the noisy biometric data. The task of tolerance value ($\beta$) is to prevent the imposter attempts to open the vault. Even if $H = N + 1$ is sufficient to reconstruct the polynomial the condition $H \geq \beta$ is enforced for the access. But the high values of $\beta$ can restrict the genuine users from decoding the vault. Hence, the choice of $\beta$ must be made to achieve the requisite error (FAR/FRR) in the authentication system.

In case $H > \beta$ and $H > N+1$ as well, any $N+1$ points from $H$ can be taken for the reconstruction of the polynomial. Let $\{\theta_H, P(\theta_H)\}$ be the set of ordered pairs corresponding to the points with $H > \beta$ and let $\{\theta_{N+1}, P(\theta_{N+1})\}$ be the candidate points selected for the reconstruction of the polynomial $p$.

The reconstruction is done using Lagrange's interpolation and the reconstructed polynomial $P^*(x)$ is obtained as

$$\begin{aligned} P^*(x) &= \frac{(x-\theta_2)(x-\theta_3)\cdots(x-\theta_{N+1})}{(\theta_1-\theta_2)(\theta_1-\theta_3)\cdots(\theta_1-\theta_{N+1})} \\ &\quad \times P(\theta_1) + \frac{(x-\theta_1)(x-\theta_3)\cdots(x-\theta_{N+1})}{(\theta_2-\theta_1)(\theta_2-\theta_3)\cdots(\theta_2-\theta_{N+1})} \\ &\quad \times P(\theta_2) + \cdots \frac{(x-\theta_1)(x-\theta_3)\cdots(x-\theta_N)}{(\theta_{N+1}-\theta_1)(\theta_{N+1}-\theta_3)\cdots(\theta_2-\theta_N)} \\ &\quad \times P(\theta_{N+1}). \end{aligned} \tag{4}$$

The reconstructed polynomial $P^*(x)$ using Lagrange's interpolation in (4) can also be represented as

$$P^*(X) = C_N^* X^N + C_{N-1}^* X^{N-1} + \cdots + C_0^*. \tag{5}$$

The reconstructed coefficients $\{C_0^*, C_1^*, C_2^* \cdots C_N^*\}$ help recover the secret binary bits by applying the method in reverse order as discussed in Section 3.1. The Antilog (base 2) transformation of all the coefficients will yield the decimal representations which are converted to binary equivalents. Each of the binary equivalents $C^*$ is of length 49 with the first bit being the CRC parity bit.

A check is made to see whether the parity bit is changed during the reconstruction of the polynomial. This check is about finding whether the binary equivalent is equal to the original one. If this check fails, it may be due to the noisy biometric data or due to the coefficient approximation by Lagrange's interpolation in (5). In this case, we examine other candidates in the set $\{\theta_H, P(\theta_H)\}$ and reconstruct the coefficients $\{C_0^*, C_1^*, C_2^* \cdots C_N^*\}$ again using (5). If none of the candidates is unable to reconstruct the original coefficients the authentication failure occurs and the user is identified to be an imposter. Finally, the converted bits (the binary equivalent) are concatenated to form the original secret key. The decoding of the vault is shown in Figure 4.

## 4. Experiments and Results

The performance of the proposed vault is ascertained by making rigorous experiments on several standard databases of different biometrics. A random binary string of 392 bits is generated as the random key (or message), which is used to calculate the polynomial coefficients. As the minutiae points of the fingerprint have been employed already for the fuzzy vault, the motivation of the proposed scheme is to evaluate the fuzzy vault on other biometric modalities using the textural features. We will enumerate the following strategies for the implementation of our fuzzy vault.

(1) Only one impression from the enrolled images of each user in the database is employed for encoding the vault and the rest are used for testing. In all the experiments the parameters of the vault are taken as follows: 392 randomly generated secret binary bits, 8 coefficients chosen for the 7 degree polynomial, 90 features selected from K-L transform for encoding of the vault, and 910 chaff points added to the original projections.

(2) Having done the encoding with one sample, other enrolled samples of the same user are recalled to encode the vault and other enrolled samples of the same user are recalled to open the vault for testing the genuine access and those of the different users are recalled to open the vault for testing the imposter access. The authentication failure of the genuine cases is marked as false rejection (FR) whereas the successful attempts of the imposter cases are marked as false acceptance (FA). For example, a 100 user database with 6 genuine attempts per user (two from each 3 enrolled samples) a total of 600 ($100 \times 6$) genuine attempts can be made. Similarly, we can have 891 ($297 \times 3$) imposter attempts per user ($99 \times 3 = 297$ images from 99 users) and hence 89100 ($891 \times 100$) in the whole database.

*4.1. Fingerprint Based Vault.* Fingerprint is a good old biometric trait for the personal authentication and its minutiae features have also found a place in the fuzzy vault scheme [2–4]. However, the proposed vault is intended to pursue the textural features from the fingerprints obtained with the application of Gabor filterbank, as detailed in [31]. Here we take recourse to the publically available FVC 2004 DB1 database, having 100 users with three samples each. The core point is detected as in [31] and ROIs are cropped using the core point as the centre point. The detection of core point itself is a challenging task and many enrolled sample images get rejected due to the false core point. A sample image from the database and the corresponding ROI are shown in Figure 5.

The cropped ROI is of size $153 \times 153$ while the original fingerprint image is of size $640 \times 480$. We create multiple Gabor filters of the size $33 \times 33$ with mean $\mu = 0$, sigma $\sigma = 5.6569$, and orientations $(\text{ang} \times (\pi/8))^0$, where ang $= 0, 1, 2 \cdots 7$. The Gabor filters at each orientation are convolved with ROIs and the real parts of this convolution are divided into nonoverlapping windows of size $15 \times 15$. A feature vector of size 832 ($104 \times 8$) is generated. In order to test the performance of the extracted features, the database is divided into two training images and one test image. Next, genuine and imposter scores are generated using the Euclidean distance, shown in Figure 6(a). For use in fuzzy vault, the extracted features are transformed using K-L transform to the reduced feature vector of size 90. The other parameters of the fingerprint based fuzzy vault are given in Table 6. Table 1 shows the value of FAR and FRR for varying values of tolerance. The ROC curve for FAR versus GAR (100-FRR) is shown in Figure 6(b).

*4.2. Palmprint Based Vault.* Despite the current popularity of the palmprint as a biometric trait only a few palmprint based cryptosystems exist in the literature [18, 23]. However, there is no attempt on utilizing the palmprint features in the

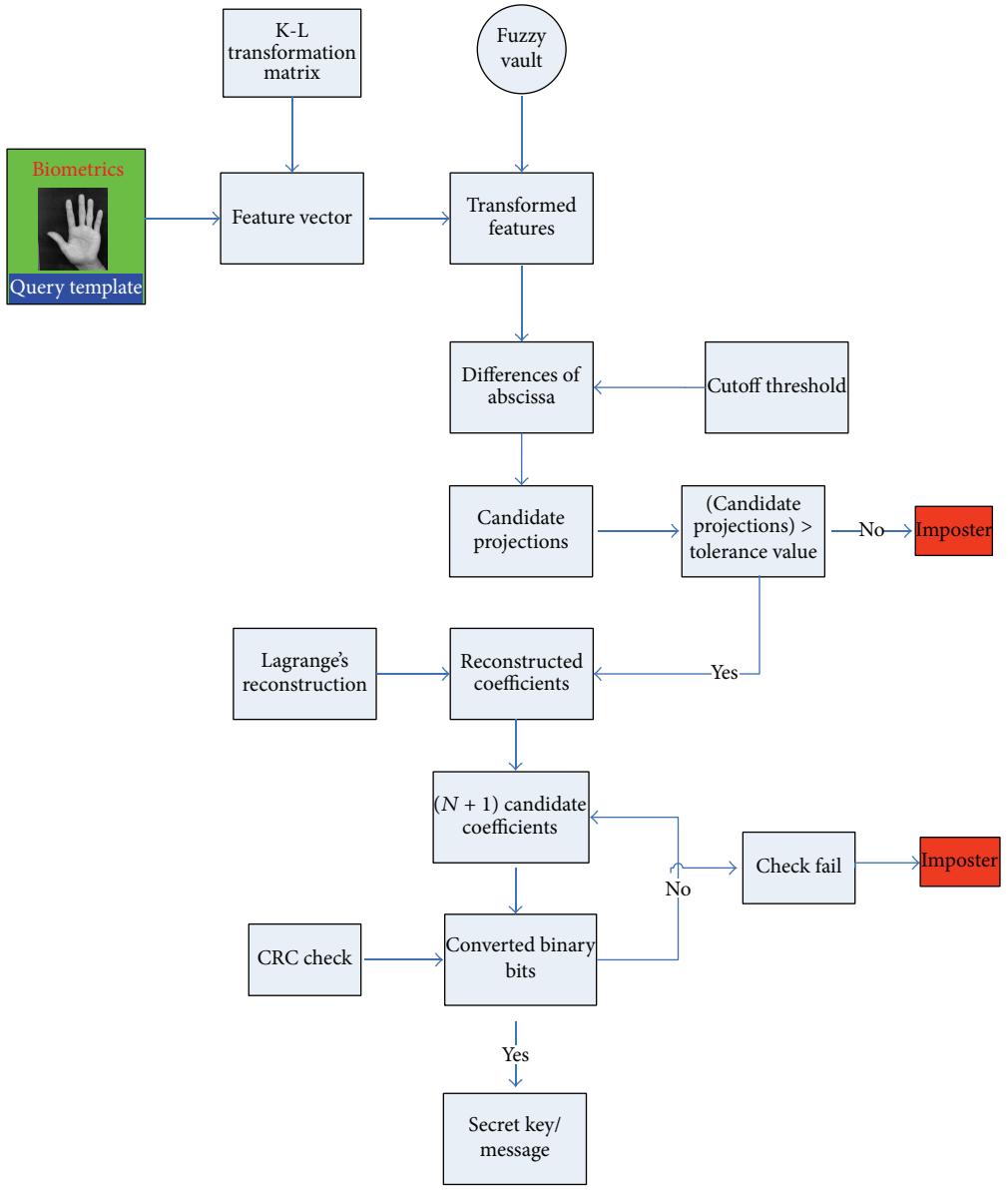


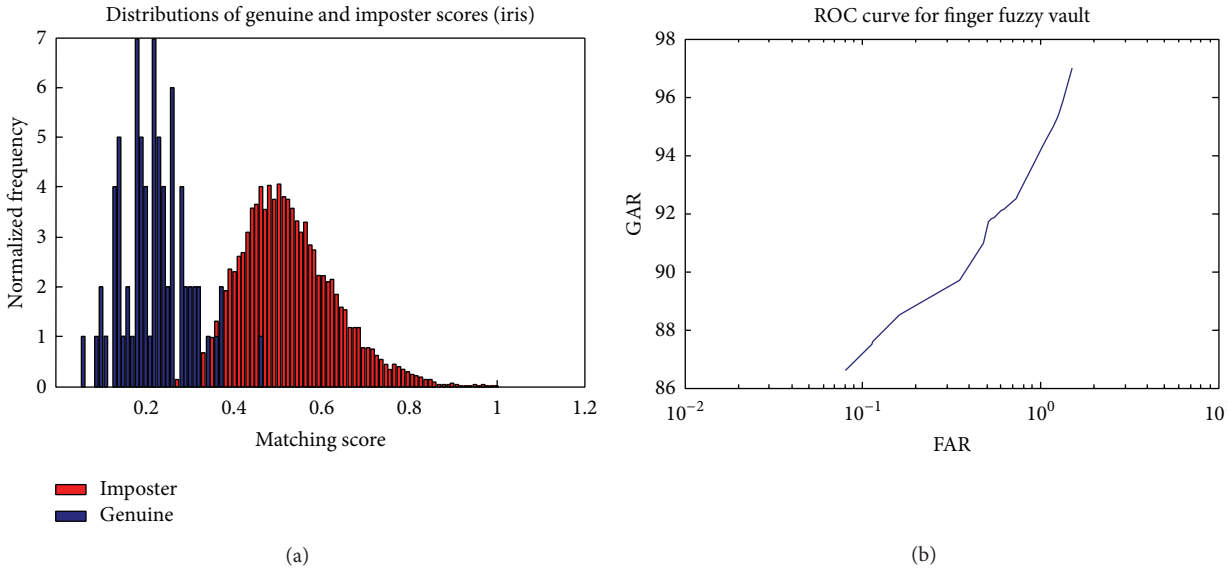

Figure 4: Decoding of the vault.

(a) (b)

Figure 5: (a) Sample image from FVC 2004 DB1 database, (b) ROI cropped from core point.

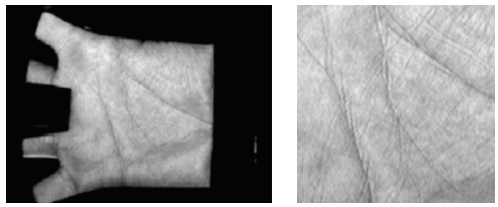
polynomial based fuzzy vault approach. We therefore embark on the palmprint features to evaluate the polynomial based fuzzy vault scheme. The database for the palmprint owes it allegiance to the publically available PolyU V2 [33]. The ROI and feature extraction method are the same as detailed in [27].

The palmprint image and the extracted ROI are shown in Figure 7. The palmprint images of size 384 × 384 are cut into ROIs of size 128 × 128. Multiple Gabor filters each of the size 35 × 35 with mean $\mu = 0.0916$, and sigma $\sigma = 5.6179$ with orientations 0°, 45°, 90°, and 135° are convolved with ROIs and the resulting real Gabor images are down sampled to 91 × 91. The real Gabor images are ROIs are then divided into nonoverlapping windows of size 7 × 7 and the mean values of these windows are stored as a Gabor feature vector of size 676 (169 × 4). In order to test the performance of the Gabor features, the PolyU database of 150 users and 5 samples each is divided into 3 training and 2 test images for each user.




(a) (b)

Figure 6: (a) Score distribution in FVC 04 database, (b) ROC of fingerprint based fuzzy vault.



(a) (b)

Figure 7: (a) Sample image from PolyU database V2, (b) corresponding ROI image.

Table 1: Performance of the fuzzy vault based on fingerprint FVC 2004 DB1 database (1 template 2 queries).

| Tolerance | 15 | 16 | 17 | 18 | 19 | **20** | 21 | 22 | 23 | 24 |
|---|---|---|---|---|---|---|---|---|---|---|
| FAR (%) | 1.5 | 1.26 | 1.12 | 0.95 | 0.72 | **0.51** | 0.48 | 0.35 | 0.16 | 0.08 |
| FRR (%) | 3.0 | 4.56 | 5.21 | 6.0 | 7.5 | **8.3** | 9.0 | 10.3 | 11.5 | 13.4 |

The genuine and imposter scores are computed using the Euclidean distance based classifier, as shown in Figure 8(a).

For the palmprint based fuzzy vault, 90 significant features are selected out of 676 Gabor features for the polynomial projection using K-L transform. The parameters of the vault are given in Table 6. Two sets of experiments are conducted on PolyU database, with the first set involving 150 users with 3 samples per user. Out of the 3 enrolled images, one image is randomly selected for encoding the vault (template) and the rest 2 images are kept for testing (query). Table 2 shows the FAR and FRR values for this experiment with the varying values of tolerance. Its ROC is shown in Figure 8(b).

The next set of experiments makes use of samples per user. One sample is embarked for encoding the template and the rest 4 samples are for the query. The FAR and FRR obtained from this experiment are given in Table 3.

Table 2: Performance of the fuzzy vault based on the 150 users palmprint database (1 template 2 queries).

| Tolerance | 17 | 18 | 19 | 20 | 21 | **22** | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|---|---|
| FAR (%) | 7.48 | 4.58 | 2.72 | 1.56 | 0.86 | **0.46** | 0.22 | 0.10 | 0.04 | 0.02 |
| FRR (%) | 2.0 | 3.0 | 4.33 | 5.00 | 7.0 | **7.33** | 9.0 | 10.0 | 11.33 | 14.33 |

Table 3: Performance of the fuzzy vault based on 150 users palmprint database (1 template 4 queries).

| Tolerance | 19 | 20 | 21 | 22 | 23 | **24** | 25 | 26 | 27 | 28 |
|---|---|---|---|---|---|---|---|---|---|---|
| FAR (%) | 10 | 6.52 | 3.99 | 2.28 | 1.25 | **0.65** | 0.32 | 0.16 | 0.07 | 0.03 |
| FRR (%) | 4.83 | 5.66 | 6.66 | 7.16 | 7.83 | **8.66** | 10.33 | 11.83 | 13.83 | 14.66 |

The corresponding ROC is shown in Figure 8(c). It can be observed that, increase in the number of query templates has very less effect on the proposed vault as reflected in FAR of 0.65% for FRR of 8.66%.

*4.3. Iris Based Vault.* Another set of experiments is carried out on the publically available CASIA I iris database [34] having 108 users with 3 samples per user which is the standard benchmark [35] for the evaluation of iris. The image normalization and Log Gabor based feature extraction are the same as in [30]. A sample iris image and the normalized enhanced iris strip are shown in Figures 9(a) and 9(b). The Log Gabor filter has a central frequency of 18 and radial bandwidth ratio of 0.55 [30].

The enhanced iris strip of size $50 \times 512$ is divided into windows of size $7 \times 7$ and mean of each window is taken as a feature leading to 522 features, which are reduced to 90 using K-L transform and the reduced features encode the vault. The genuine and imposter scores are generated by dividing the database into 2 training and 1 test images. The distribution of scores is shown in Figure 10(a). The parameters of the iris

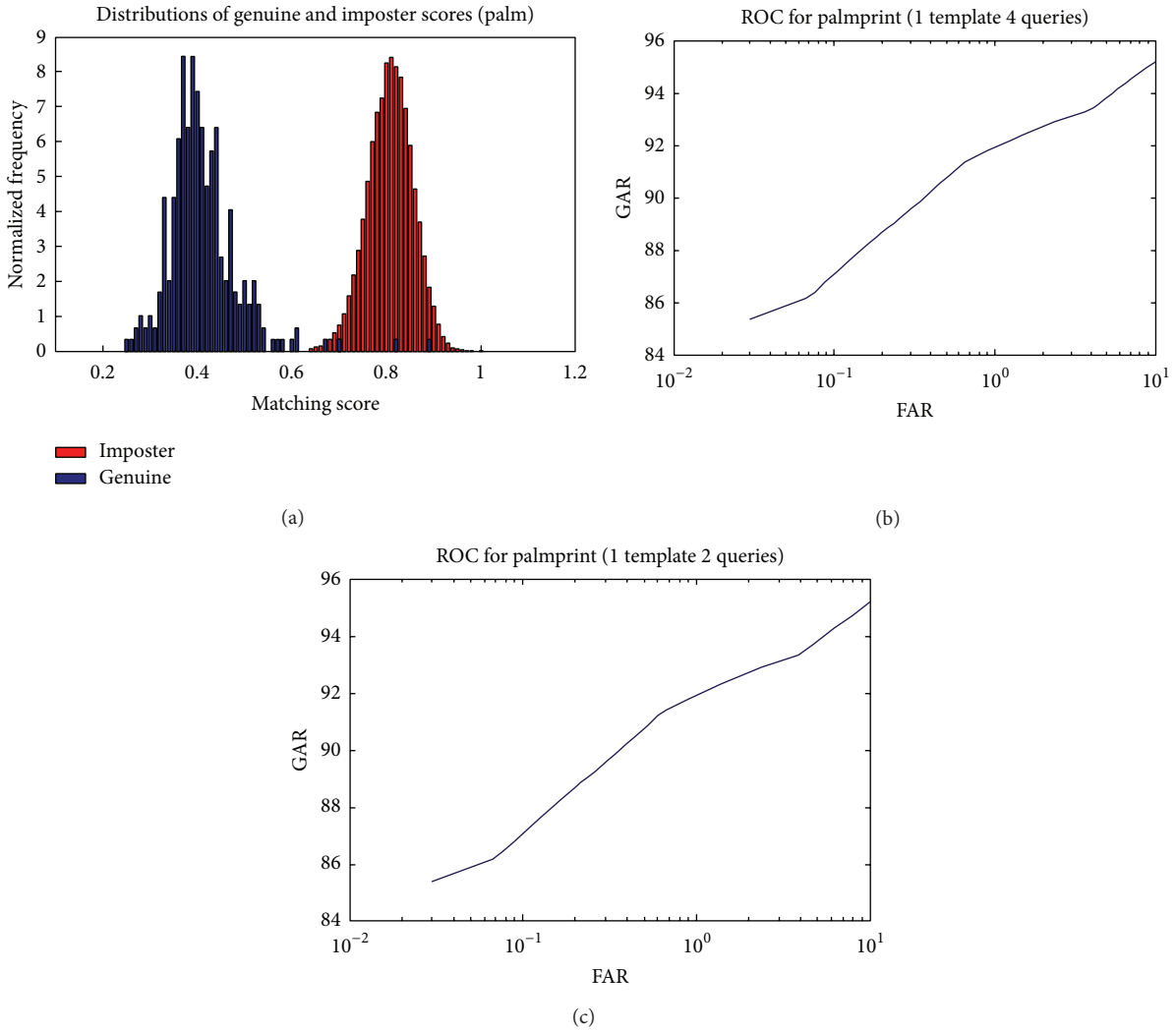


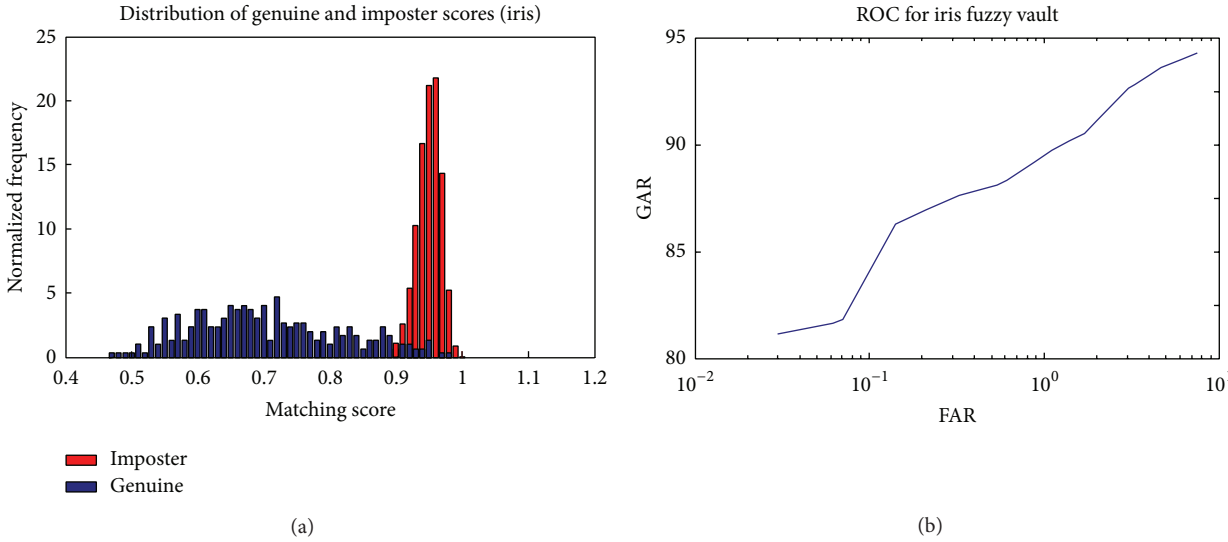

FIGURE 8: (a) Score distribution in PolyU V2 database, (b) ROC of palmprint fuzzy vault with 1 template and 4 queries, and (c) ROC of the same vault fuzzy vault with 1 template and 2 queries.


FIGURE 9: (a) Iris sample image, (b) iris normalized strip enhanced with Log Gabor filter.

based fuzzy vault are given in Table 6. Table 4 presents FARs and FRRs for the varying values of tolerance. Figure 10(b) shows the ROC generated from these error rates.

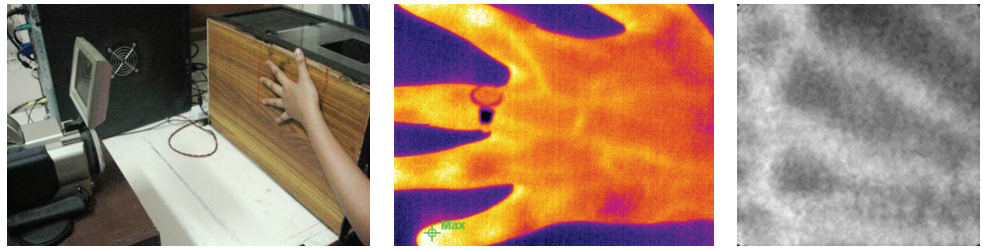
*4.4. Hand Vein Based Vault.* To test the performance of the proposed vault on a variety of biometric modalities, the use of the infrared thermal hand vein images is also made. Beneath the skin, vein patterns are too harder to intercept for an intruder; hence is a safer biometric trait. Realizing the inherent potential of the infrared thermal hand vein patterns as a biometric trait, these are some works on its use for authentication [36–38].

Since there is no database of the infrared thermal hand veins patterns, a database has been created at Biometrics Research Laboratory, IIT, Delhi. This database consists of infrared thermal hand vein images of 100 users with three




(a) (b)

Figure 10: (a) Score distribution in CASIA I database, (b) ROC of iris based fuzzy vault.



(a) (b) (c)

Figure 11: (a) Camera setup, (b) captured image, and (c) normalized image.

Table 4: Performance of the vault based on the 108 users iris database (1 template 3 queries).

| Tolerance | 18 | 19 | 20 | 21 | 22 | 23 | **24** | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|
| FAR (%) | 7.45 | 4.85 | 2.97 | 1.73 | 1.08 | 0.57 | **0.31** | 0.14 | 0.07 | 0.03 |
| FRR (%) | 5.75 | 6.37 | 7.45 | 9.45 | 10.30 | 11.85 | **12.46** | 13.70 | 18.24 | 18.86 |

images. The camera setup, image acquisition, and image normalization (ROI extraction) of the hand vein images are the same as in [36]. A sample image and the corresponding normalized image are shown in Figure 11. Here, the Gabor wavelet features [36] are employed for the vault implementation. The parameters used for the vein based fuzzy vault are given in Table 6.

The ROIs of size $104 \times 104$ extracted from the infrared hand vein images of size $320 \times 240$ are enhanced by Gabor wavelet filters with orientations $0^\circ$, $45^\circ$, $90^\circ$, and $135^\circ$. The real parts of the convolved images are called real-Gabor images. The real-Gabor images are divided into windows of size $8 \times 8$ and thus yielding a total of 676 ($169 \times 4$) Gabor features. Using these features, genuine and imposter scores are generated by dividing the database into 2 training and 1 test, as shown in Figure 12(a).

These features are reduced to 90 features by the application of K-L transform. The parameters of vein fuzzy vault are given in Table 6. The values of FAR and FRR for different values of threshold are given in Table 5. The corresponding ROC is shown in Figure 12(b).

## 5. Discussion

The fuzzy vault of this paper has two main features. (1) it is carried out on the feature vector extracted using Gabor filters which are robust and easy to implement and have less time complexity. In comparison, minutiae features are computationally difficult to extract, suffer from the problem of false and spurious minutiae points, and pose problems in the alignment in the fuzzy vault [4]. (2) It leads to low error rates and hence is comparable to the previous fuzzy vaults [1–4]. The fingerprint based vault generates FAR of 0.51 at FRR of 8.3, palmprint based vault yields FAR of 0.46 at of FRR: 7.33, and iris based vault gives FAR of 0.31 at FRR of 12.6. The high error rates due to fingerprint and iris based vaults are on account of features from sliding windows (see Section 4.3). Incorporating the minutiae features of fingerprint [4] and Hamming distance from iris code may produce better results [30]. However, the proposed approach

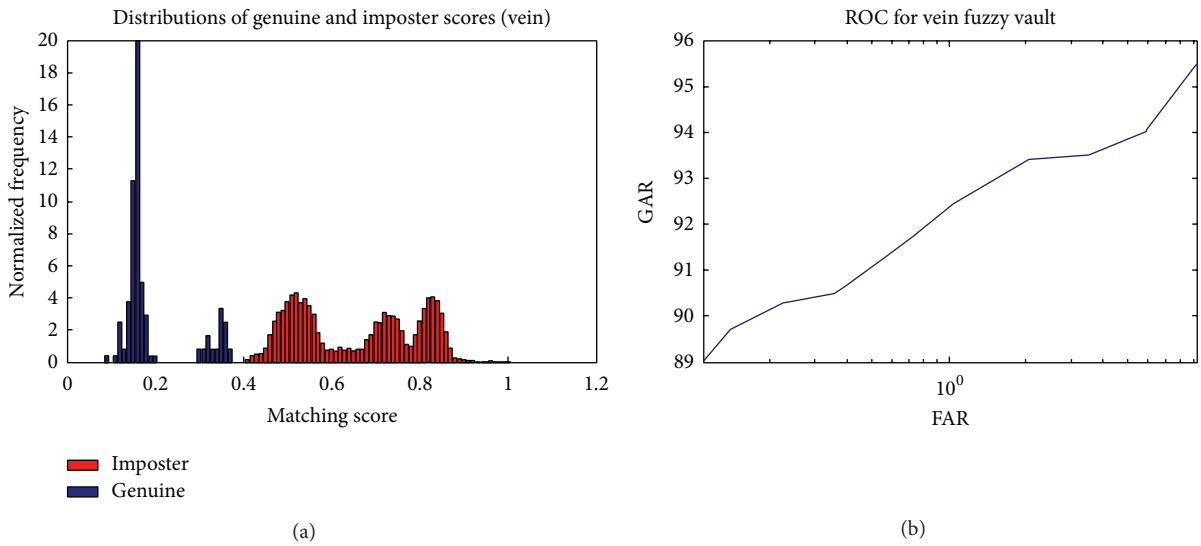



Figure 12: (a) Score distribution in IITD Vein database, (b) ROC of vein based fuzzy vault.

Table 5: Performance of the proposed fuzzy vault based on the hand vein database.

| Tolerance | 17 | 18 | 19 | 20 | 21 | **22** | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|---|---|
| FAR (%) | 9.27 | 5.8 | 3.5 | 2.07 | 1.07 | **0.64** | 0.36 | 0.23 | 0.14 | 0.11 |
| FRR (%) | 4.5 | 6.0 | 6.5 | 6.6 | 7.5 | **8.5** | 9.5 | 9.7 | 10.3 | 11 |

Table 6: Description of the parameter used in different vaults.

| Parameter | Biometric database | | | |
|---|---|---|---|---|
| | Fingerprint | Palmprint | Iris | Hand veins |
| No of users | 100 | 150 | 108 | 100 |
| No of samples per user | 3 | 5 | 4 | 3 |
| Value of cutoff threshold ($\alpha$) | 21 | 0.2 | 21 | 35 |
| Best value of tolerance ($\beta$) | 20 | 24 | 24 | 22 |

is simpler. The results reported by hand vein based vault are as follows: FAR: 0.64 and FRR: 8.5. Infrared thermal hand veins are for the first time utilized for fuzzy vault in this work. The experimental results show that hand vein based vault is comparable to fingerprint, palmprint, and iris based vaults and can serve as a benchmark for the evaluation of fuzzy vault.

The vulnerability of fuzzy vault to different attacks is addressed in [29, 39]. The issues of security related to the fuzzy vault based cryptosystem are discussed in [1, 4]. Here, we discuss the security issues to circumvent the random attacks on the proposed fuzzy vault. The degree of the polynomial $N$ is taken as 7 to hide a secret key of size 392 bits with feature vector of size 90. If 910 chaff points are added to the vault, the total number of possible combinations is ${}^{1000}_{8}\mathrm{C} \approx 2.4 \times 10^{19}$ and out of these ${}^{90}_{8}\mathrm{C} \approx 7.7 \times 10^{9}$ combinations can successfully decode the vault. The probability of decoding the vault with one combination is $(7.7 \times 10^{9}/2.4 \times 10^{19}) \approx 3.2 \times 10^{-10}$ and the number of calculations needed is $(2.4 \times 10^{19}/7.7 \times 10^{9}) \approx 3.1 \times 10^{9}$. Thus, for the polynomial of degree 7, the probability of breaking this vault is $3.2 \times 10^{-10}$. However, if the degree is reduced to 6 this probability is increased to $3.8 \times 10^{-8}$ and length of the secret key is changed to 343. The number of chaff points is chosen to be approximately 10 times greater than the genuine points.

## 6. Conclusions

The current popularity of the biometric modalities, like iris, palmprint, hand veins, and so forth, is behind the motivation to investigate the polynomial based fuzzy vault. This paper therefore presents a new scheme for the fuzzy vault based on the texture features of these traits. The prior work on the polynomial based fuzzy vault deals with the minutiae points as the biometric data. The fuzzy vault is a kind of biometric cryptosystems that spring forth from the integration of both the secret key and the biometric features, and, once this is locked in the vault, it is computationally very difficult to intrude the key or retrieve the stored features without the knowledge of any one of them.

In the proposed scheme, a new method of generating the polynomial coefficients, which can hide a secret key of 392 bits with the polynomial of degree 7, is developed. The original features from the biometric modalities are transformed using K-L transform for encoding the vault. The cutoff threshold is learned from the transformed features to separate out the chaff points from the original features. The transformation matrix and the cutoff threshold are saved and the original and the transformed features are discarded from the database for the security reasons. The proposed vault is implemented separately on a variety of biometric databases, including the publically available, fingerprint (FVC 2004), palmprint (PolyU V2), and iris (CASIAV1); and hand Veins. The performance of the proposed vault can be further

improved by using multiple biometric traits like palmprint and fingerprint or palmprint of both the palms of a user.

## Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

## References


[1] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–959, 2004.

[2] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," in *Audio- and Video-Based Biometric Person Authentication*, vol. 3546 of *Lecture Notes in Computer Science*, pp. 310–319, Springer, 2005.

[3] U. Uludag and A. K. Jain, "Securing fingerprint template: fuzzy vault with helper data," in *Proceedings of the Conference on Computer Vision and Pattern Recognition Workshops*, p. 163, New York, NY, USA, June 2006.

[4] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 744–757, 2007.

[5] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," in *Proceedings of the 6th ACM Conference on Computer and Communications Security (CCS '99)*, pp. 73–82, November 1999.

[6] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[7] C. Sautar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. K. Vijaya Kumar, "Biometric encryption," *Information Management and Computer Security*, vol. 9, no. 5, pp. 205–212, 2001.

[8] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," Cryptology Eprint Archive, Tech. Rep 235, 2006.

[9] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proceedings of the IEEE International Symposium on Information Theory*, p. 408, July 2002.

[10] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in *Proceedings of the IEEE 2nd International Conference on Biometrics: Theory, Applications and Systems (BTAS '08)*, pp. 1–6, Arlington, Va, USA, October 2008.

[11] A. Goh and D. C. L. Ngo, "Computation of cryptographic keys from face biometrics," in *Communications and Multimedia Security. Advanced Techniques for Network and Data Protection*, vol. 2828 of *Lecture Notes in Computer Science*, pp. 1–13, Springer, 2003.

[12] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[13] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 148–157, Oakland, Calif, USA, May 1998.

[14] Y. J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation," in *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 2203–2206, 2004.

[15] T. Connie, A. Teoh, M. Goh, and D. Ngo, "PalmHashing: a novel approach for cancelable biometrics," *Information Processing Letters*, vol. 93, no. 1, pp. 1–5, 2005.

[16] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of BioHashing and its variants," *Pattern Recognition*, vol. 39, no. 7, pp. 1359–1368, 2006.

[17] A. Kong, D. Zhang, and M. Kamel, "Three measures for secure palmprint identification," *Pattern Recognition*, vol. 41, no. 4, pp. 1329–1337, 2008.

[18] X. Wu, D. Zhang, and K. Wang, "A palmprint cryptosystem," in *Advances in Biometrics*, vol. 4642, pp. 1035–1042, Springer, 2007.

[19] X. Boyen, "Reusable cryptographic fuzzy extractors," in *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04)*, pp. 82–91, ACM Press, October 2004.

[20] A. Juel and M. Wttenberg, "A fuzzy vault commitment scheme," in *Proceedings of the 6th ACM conference on Computer and Communications Security*, G. Tsudik, Ed., pp. 408–412, 2002.

[21] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, NY, USA, 1968.

[22] A. Nagar and S. Chaudhury, "Biometrics based asymmetric cryptosystem design using modified fuzzy vault scheme," in *Proceedings of the 18th International Conference on Pattern Recognition (ICPR '06)*, pp. 537–540, Hong Kong, China, August 2006.

[23] A. Kumar and A. Kumar, "Development of a new cryptographic construct using palmprint-based fuzzy vault," *Eurasip Journal on Advances in Signal Processing*, vol. 2009, Article ID 967046, 2009.

[24] Y. J. Lee, K. R. Park, S. J. Lee, K. Bae, and J. Kim, "A new method for generating an invariant iris private key based on the fuzzy vault system," *IEEE Transactions on Systems, Man, and Cybernetics, B: Cybernetics*, vol. 38, no. 5, pp. 1302–1313, 2008.

[25] X. Wu, D. Zhang, and K. Wang, "A palmprint cryptosystem," in *Advances in Biometrics*, vol. 4642 of *Lecture Notes in Computer Science*, pp. 1035–1042, 2007.

[26] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-Garcia, "Cryptographic key generation using handwritten signature," in *Biometric Technology for Human Identification III*, vol. 6202 of *Proceedings of SPIE*, pp. 225–231, April 2006.

[27] D. Zhang, W.-K. Kong, J. You, and M. Wong, "Online palmprint identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, pp. 1041–1050, 2003.

[28] S. Ribaric and I. Fratric, "A biometric identification system based on eigenpalm and eigenfinger features," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 11, pp. 1698–1709, 2005.

[29] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Proceedings of the Biometrics Symposium*, pp. 1–6, Baltimore, Md, USA, September 2007.

[30] A. Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal authentication," *Pattern Recognition*, vol. 43, no. 3, pp. 1016–1026, 2010.

[31] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9, no. 5, pp. 846–859, 2000.

[32] http://en.wikipedia.org/wiki/Uniform_distribution_%28continuous%29.

[33] "The PolyU Palmprint Database ver.2.0," http://www.comp.polyu.edu.hk/~biometrics.

[34] CASIA IRIS Database, 2008, http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp.

[35] H. Proença and L. A. Alexandre, "Toward noncooperative iris recognition: a classification approach using multiple signatures," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 607–612, 2007.

[36] A. Kumar, M. Hanmandlu, and H. M. Gupta, "Online biometric authentication using hand vein patterns," in *Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA '09)*, Ottawa, Canada, July 2009.

[37] L. Wang, G. Leedham, and S.-Y. Cho, "Infrared imaging of hand vein patterns for biometric purposes," *IET Computer Vision*, vol. 1, no. 3-4, pp. 113–122, 2007.

[38] C.-L. Lin and K.-C. Fan, "Biometric verification using thermal images of palm-dorsa vein patterns," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 2, pp. 199–213, 2004.

[39] A. Kholmatov and B. Yanikoglu, "Realization of correlation attack against the Fuzzy Vault scheme," in *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, vol. 6819 of *Proceedings of SPIE*, January 2008.