

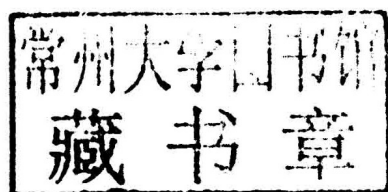


Machine Vision and its Applications

Martha Lesley

Machine Vision and its Applications

Edited by **Martha Lesley**



New Jersey

Published by Clanrye International,
55 Van Reypen Street,
Jersey City, NJ 07306, USA
www.clanryeinternational.com

Machine Vision and its Applications
Edited by Martha Lesley

© 2015 Clanrye International

International Standard Book Number: 978-1-63240-332-2 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Copyright for all individual chapters remain with the respective authors as indicated. A wide variety of references are listed. Permission and sources are indicated; for detailed attributions, please refer to the permissions page. Reasonable efforts have been made to publish reliable data and information, but the authors, editors and publisher cannot assume any responsibility for the validity of all materials or the consequences of their use.

The publisher's policy is to use permanent paper from mills that operate a sustainable forestry policy. Furthermore, the publisher ensures that the text paper and cover boards used have met acceptable environmental accreditation standards.

Trademark Notice: Registered trademark of products or corporate names are used only for explanation and identification without intent to infringe.

Printed in China.

Machine Vision and its Applications

Preface

Machine Vision is exactly what it entails, the ability of a machine to 'see', though the process might differ according to type and application. Distantly related to computer vision, machine vision is increasingly used to provide services equivalent to that of a human supervisor and analyst, that is, using technology to provide image based applications for processes like automatic inspection and robotic guidance in industries. As machines are increasingly becoming part and parcel of our daily lives, the scope of machine vision is ever-increasing. Though standardization is slowly becoming the norm, there are still various methods of using machine vision. As digital image processes are used to extract information, different types of lenses, cameras and lighting are used as required. Machine is not just restricted to 2D images but also infrared bands and X-ray imaging as well as 3D images. Such differentiated methods speak for the ever changing instruments of machine vision. Such an essential part of the industrial process has a constantly increasing market for its varied applications. The future is limitless for machine vision, from agriculture to robotics. But there is also trepidation about such advanced uses as it can potentially take away jobs from the workforce.

The book focuses on the various applications, markets and changing technology in the field known as machine vision. I would like to thank those who have contributed to this field of work for making this book possible and my family for their constant support.

Editor

Contents

	Preface	VII
Chapter 1	A New Scheme for the Polynomial Based Biometric Cryptosystems Amioy Kumar, M. Hanmandlu and Hari M. Gupta	1
Chapter 2	Performance Evaluation of Noise Reduction Filters for Color Images through Normalized Color Difference (NCD) Decomposition Fabrizio Russo	14
Chapter 3	Active Object Recognition with a Space-Variant Retina Christopher Kanan	25
Chapter 4	Affine-Invariant Feature Extraction for Activity Recognition Samy Sadek, Ayoub Al-Hamadi, Gerald Krell and Bernd Michaelis	35
Chapter 5	LoCoBoard: Low-Cost Interactive Whiteboard Using Computer Vision Algorithms Christophe Soares, Rui S. Moreira, José M. Torres and Pedro Sobral	42
Chapter 6	Resection-Intersection Bundle Adjustment Revisited Ruan Lakemond, Clinton Fookes and Sridha Sridharan	55
Chapter 7	Fast Exact Nearest Neighbour Matching in High Dimensions Using d-D Sort Ruan Lakemond, Clinton Fookes and Sridha Sridharan	63
Chapter 8	Multimodal Markov Random Field for Image Reranking Based on Relevance Feedback Ricardo Omar Chávez, Hugo Jair Escalante, Manuel Montes-y-Gómez and Luis Enrique Sucar	71
Chapter 9	Towards Understanding the Formation of Uniform Local Binary Patterns Olli Lahdenoja, Jonne Poikonen and Mika Laiho	87
Chapter 10	A Robust Illumination Normalization Method Based on Mean Estimation for Face Recognition Yong Luo, Ye-Peng Guan and Chang-Qi Zhang	107

Chapter 11	Visible and Infrared Face Identification via Sparse Representation Pierre Buyssens and Marinette Revenu	117
Chapter 12	Novel Approach for Rooftop Detection Using Support Vector Machine Hayk Baluyan, Bikash Joshi, Amer Al Hinai and Wei Lee Woon	127
Chapter 13	Area Optimized FPGA-Based Implementation of The Sobel Compass Edge Detector Sanjay Singh, Anil Kumar Saini, Ravi Saini, A. S. Mandal, Chandra Shekhar and Anil Vohra	138
Chapter 14	Deformable Contour-Based Maneuvering Flying Vehicle Tracking in Color Video Sequences Samira Sabouri, Alireza Behrad and Hassan Ghassemian	144
Chapter 15	Vision Measurement Scheme Using Single Camera Rotation Shidu Dong	158
Chapter 16	New Brodatz-Based Image Databases for Grayscale Color and Multiband Texture Analysis Safia Abdelmounaime and He Dong-Chen	165
Chapter 17	Local Stereo Matching Using Adaptive Local Segmentation Sanja Damjanović, Ferdinand van der Heijden and Luuk J. Spreeuwiers	179

Permissions

List of Contributors

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

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, *Bio-script*. 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 et al. [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, θ) [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 $T = \{t_1, t_2, \dots, t_r\}$ 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

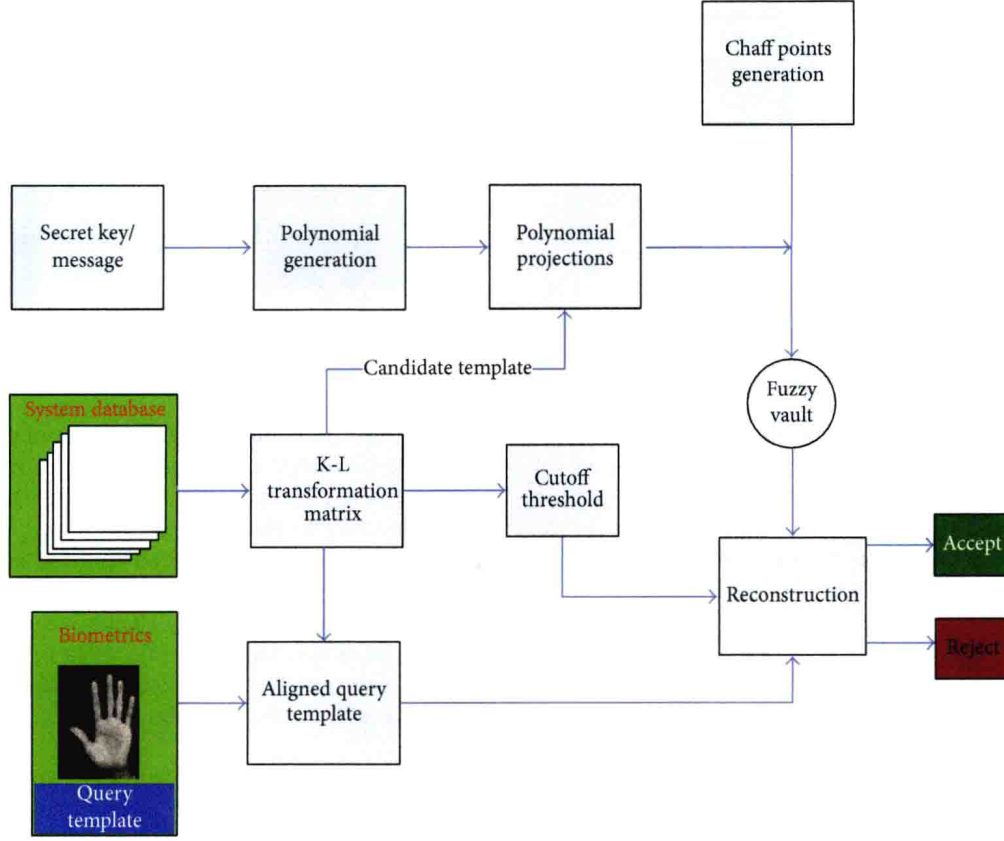


FIGURE 1: Block diagram of the complete system.

$P(x) = a_0 + a_1x + \dots + a_{(n-1)}x^{N-1}$ 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 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 $T' = \{t'_1, t'_2 \dots t'_r\}$ of " r " elements. If T' overlaps substantially with T , the user can retrieve many original points from 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

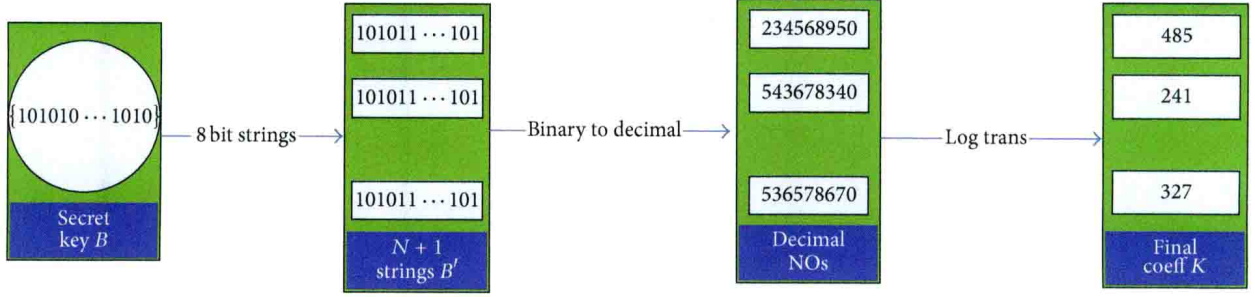


FIGURE 2: Block diagram for generating polynomial coefficients.

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 (α) and the tolerance value (β). 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 $\{\theta_1, \theta_2 \dots \theta_k\}^T$, whose projections on the polynomial P of degree N form the projection set $P_r = \{P(\theta_1), P(\theta_2) \dots P(\theta_k)\}^T$. Next, $N + 1$ coefficients of P computed using the secret key (detailed in Section 4.1) are saved as $K = \{C_0, C_1, C_2 \dots C_N\}$. The elements of the projection set are obtained as

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

The ordered pairs $\{\theta_i, P(\theta_i)\}; i = 1, 2, 3, \dots, k$, are made up of point θ_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 $\delta_i; i = 1, 2, 3, \dots, k$, and the generated random numbers do not coincide with any of the original k features. For example, considering δ_i as mean and $[\delta_{i+1} - \delta_i]$ as variance, we can generate 10 random numbers for each data point δ_i resulting in 900 chaff points corresponding to 90 transformed feature points.

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

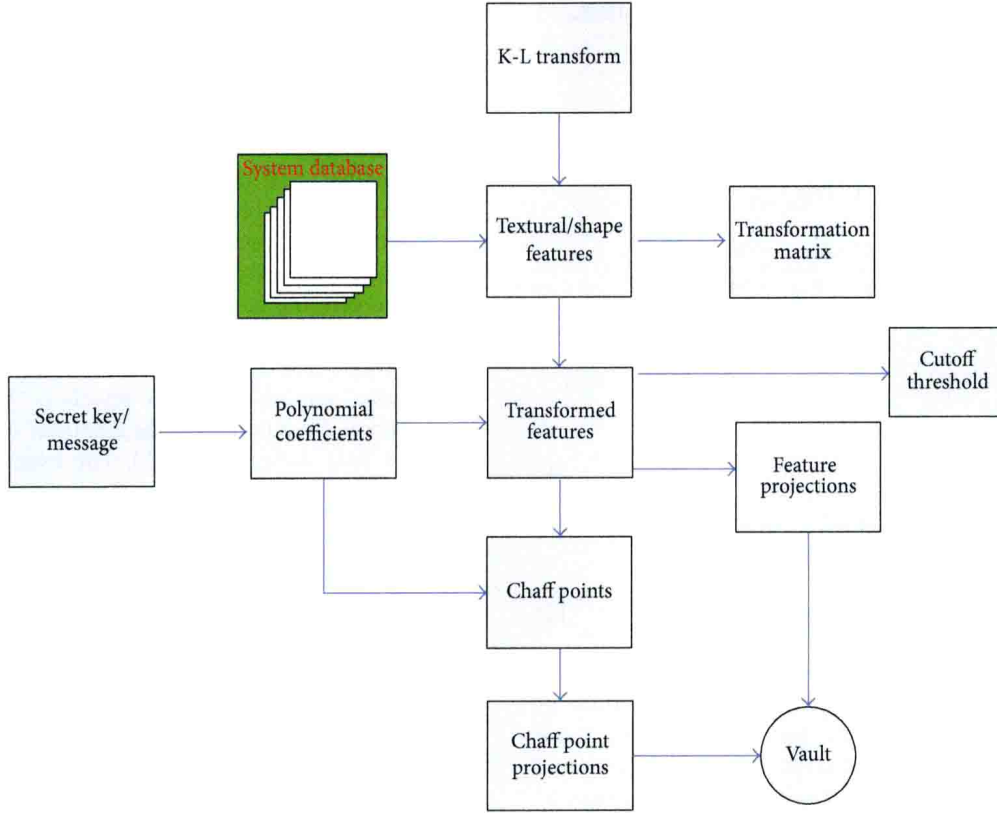


FIGURE 3: Encoding of the vault.

from μ_{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 θ_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 (α), tolerance value (β), 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 (α), learned from the transformed features $\{\delta\}_{k \times 1}$, and the tolerance value (β) which is fixed according to the tradeoff in the error rates (FAR/FRR).

The query feature vector $q = \{q_1, q_2, q_3 \dots q_{N1}\}$ undergoes the K-L transformation $\{V_k^T\}_{k \times N1}$, to yield the transformed query feature vector $Q = \{Q_1 Q_2 \dots Q_k\}$ 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 α 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 $K = \{C_0, C_1, C_2 \dots C_N\}$ 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 (β) 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 β can restrict the genuine users from decoding the vault. Hence, the choice of β 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

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

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 (100×6) genuine attempts can be made. Similarly, we can have 891 (297×3) imposter attempts per user ($99 \times 3 = 297$ images from 99 users) and hence 89100 (891×100) 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 153×153 while the original fingerprint image is of size 640×480 . We create multiple Gabor filters of the size 33×33 with mean $\mu = 0$, sigma $\sigma = 5.6569$, and orientations $(\text{ang} \times (\pi/8))^0$, where $\text{ang} = 0, 1, 2 \cdots 7$. The Gabor filters at each orientation are convolved with ROIs and the real parts of this convolution are divided into nonoverlapping windows of size 15×15 . A feature vector of size 832 (104×8) 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 ($100 - \text{FRR}$) 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

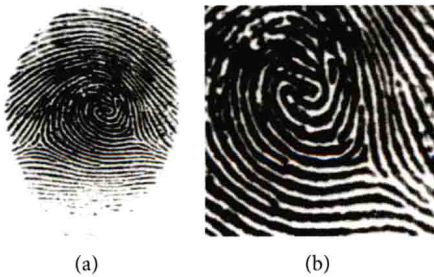
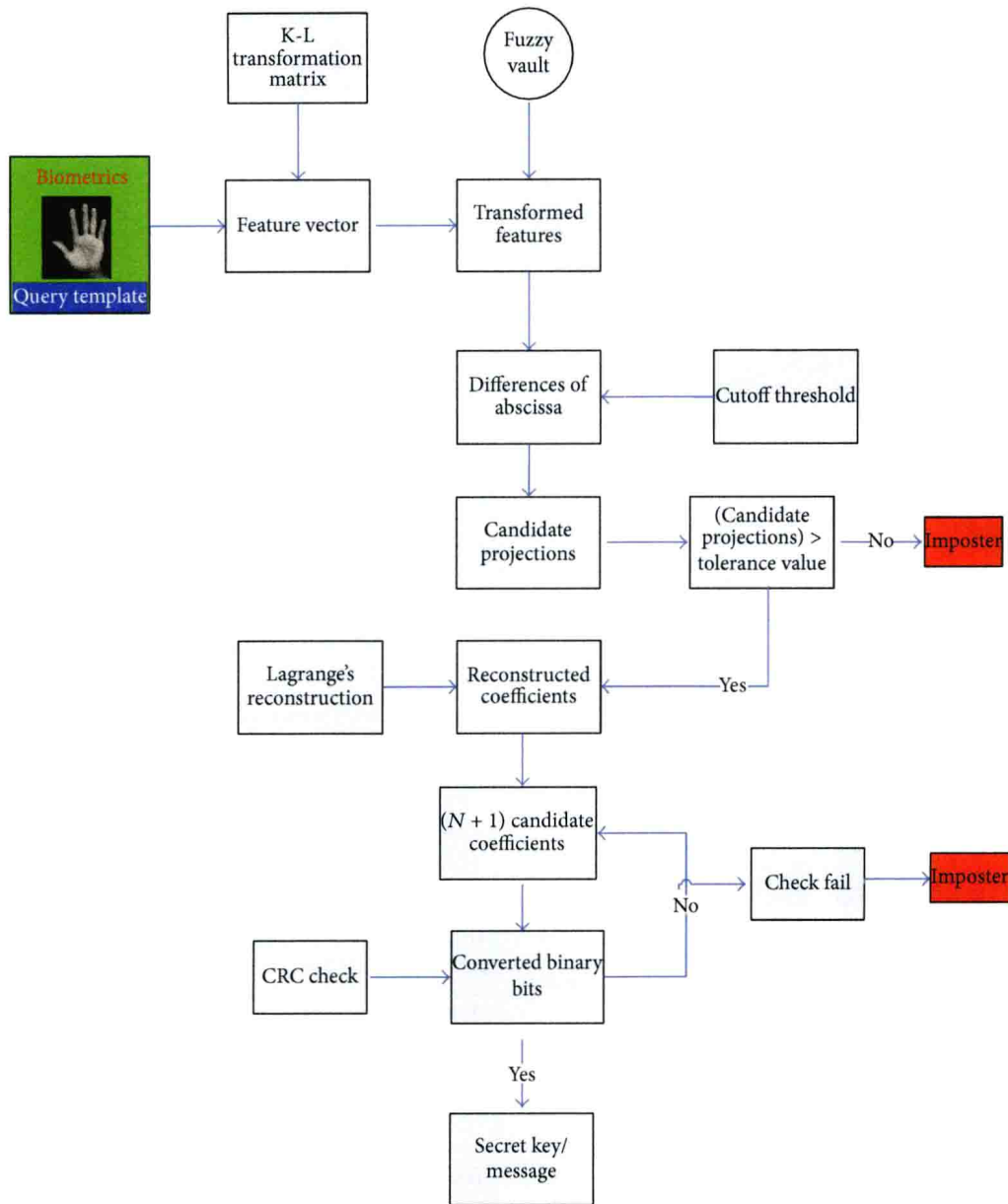
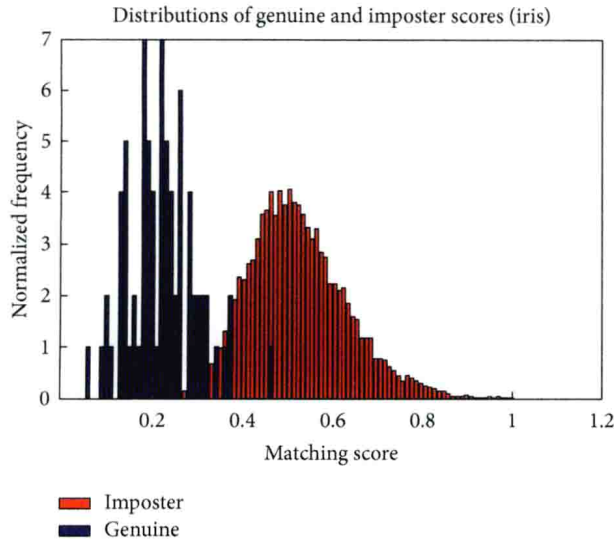


FIGURE 5: (a) Sample image from FVC 2004 DB1 database, (b) ROI cropped from core point.

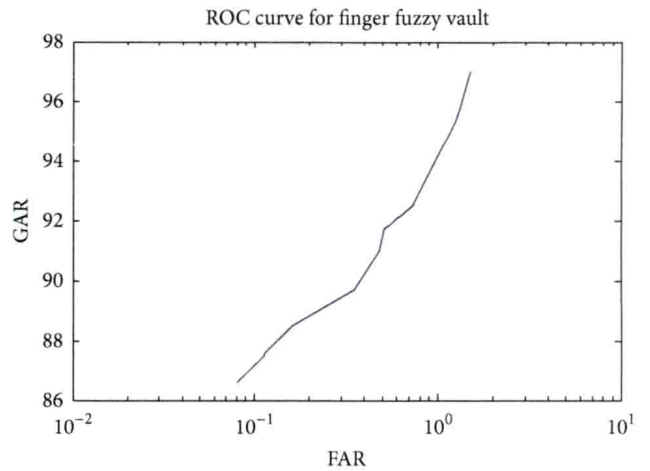
polynomial based fuzzy vault approach. We therefore embark on the palmprint features to evaluate the polynomial based

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 $676 (169 \times 4)$. 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.

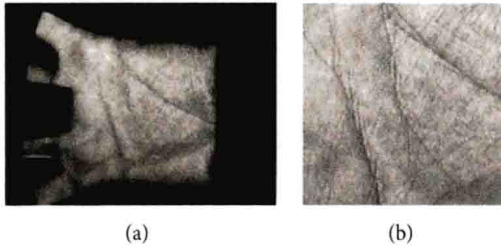


(a)



(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 50×512 is divided into windows of size 7×7 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