B.TECH. PROJECT REPORT

On

Fingerprint Based Biometric Cryptosystem using Fuzzy Vault Technique

By

Ity Agrawal

160002018

DISCIPLINE OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY INDORE

DECEMBER 2019

Fingerprint Based Biometric Cryptosystem using Fuzzy Vault Technique

A PROJECT REPORT

Submitted in partial fulfillment of the

requirements for the award of the degrees

of

BACHELOR OF TECHNOLOGY

in

ELECTRICAL ENGINEERING

Submitted by :

Ity Agrawal

Guided by :

Dr. Surya Prakash
Associate Professor, Discipline of Computer Science and Engineering, IIT Indore

DISCIPLINE OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY INDORE
DECEMBER 2019

Candidate's Declaration

I hereby declare that the project entitled **Fingerprint Based Biometric Cryptosystem using Fuzzy Vault Technique** submitted in partial fulfillment for the award of the degree of Bachelor of Technology in **Discipline of Electrical Engineering** completed under the supervision of **Dr.Surya Prakash**, Associate professor, Discipline of Computer Science and Engineering, IIT Indore is an authentic work.
Further, I declare that I have not submitted this work for the award of any other degree elsewhere.

Ity Agrawal

Certificate by BTP Guide

It is certified that the above statement made by the student is correct to the best of my knowledge.

Dr. Surya Prakash
Associate Professor
Discipline of Computer Science and Engineering
IIT INDORE

Preface

This report on **Fingerprint Based Biometric Cryptosystem using Fuzzy Vault Technique** is prepared under the guidance of **Dr. Surya Prakash**.

The report intends to give a detailed design and analysis of a biometric protection technique, known as fuzzy vault. Furthermore, this report attempts to clearly explain the enhancements applied to the existing technique to reduce the complexity of the technique and compare the results obtianed to the results on fuzzy vault proposed earlier in the literature.

I have tried to the best of my abilities and knowledge to explain the proposed method in a lucid manner. The results obtained with the present work are also included in this report. I have also added the comparison of the present work with some of the existing works in this direction.

Ity Agrawal
B.Tech. IV Year
Discipline of Electrical Engineering
IIT Indore

Acknowledgments

I would like to take this opportunity to express my gratitude to the people who have been instrumental in the successful completion of my course of research.

I would like to express my sincere gratitude to **Prof. Dr. Surya Prakash**, my project supervisor, for valuable suggestions and keen interest through out the progress of my course of research work.

I would also like to take this opportunity to thank **Mr. Vivek Singh Baghel**, Ph.D. scholar in Discipline of Computer Science and Engineering. It was his generous support that helped me learn the fundamentals and his positive temperament that made even the demotivating situation easy to sail through.

I would like to acknowledge IIT Indore for providing all necessary research infrastructures required for undertaking the project.

Ity Agrawal
B.Tech. IV Year
Discipline of Electrical Engineering
IIT Indore

Abstract

Secure systems are required to fight with the rising magnitude of identity theft in our society. Earlier password based systems were used for authentication purposes. However, they were not that secure as the password can be lost, stolen or forgotten by anyone. Thus, a need arisen for the requirement of more secured authentication systems and then came the biometric systems. In biometrics, the use of distinctive biological and behavioral characteristics, that cannot be copied or changed, are used. But the main problem that came up with these systems is the security of the biometric template that is stored in the database. Biometric cryptosystems turn out to be the best possible solution for this problem. In these systems, only a transformed version of the template is stored in the database rather than storing the original template. Several biometric cryptosystems have been proposed in the literature and the Fuzzy vault construct proposed by Juels and Sudan [1] is an instance of such systems. We here present the Fuzzy vault scheme based on fingerprint minutiae as described in [2] but with significant modifications.

We have used different alignment and filtering techniques as compared to the proposed methodology in [2]. In the Fuzzy vault, only the transformed version of the template is stored in the database rather than storing the original template with minutiae information. Thus, aligning the query fingerprint with the original template is a very challenging task. In [2] high curvature points are extracted from the orientation field and stored as helper data in the database to assist in the alignment of fingerprint images. Instead of using this alignment method, we have used the PCA technique to align the template and query minutiae accurately. PCA technique when applied on a given fingerprint dataset, gives the two uncorrelated orthogonal vectors known as principal components one and two respectively. This is represented in Figure:3.4. The whole image is rotated with a singular point as a reference such that PC_1 is aligned to the vertical axis. This technique is giving good alignment results. Moreover, it does not require any helper data to be stored in the database, consuming less computational time and much simpler for implementation.

At the time of decoding the vault, we have also included the relative distance minutiae matching algorithm as described in Section 3.5. This method performed after the coarse filtering steps further reduces the number of chaff points and thus, reduces the size of the unlocking set. As a result, fewer decoding sets combinations are formed and the total time complexity of the system is reduced further.

We have demonstrated the performance of the Fuzzy vault implementation on two different fingerprint databases (FVC2002 DB1 and FVC2002 DB2). We have also compared our results with the earlier proposed fingerprint based Fuzzy vault systems. By using multiple fingerprint impressions during enrollment and authentication, the performance of the system can be improved further is also shown.

Abbreviations

CRC: Cyclic Redundancy Check

PCA: Principal Component Analysis

AHE: Adaptive Histogram Equalization

AES: Advanced Encryption Standard

GAR: Genuine Acceptance Rate

FRR: False Rejection Rate

FAR: False Acceptance Rate

Contents

List of Figures

List of Tables

Chapter 1

Introduction

A person's physiological or behavioral characteristics, known as biometrics, are important and vital methods that can be used for identification and verification. Earlier passwords were used for authentication purpose but they were not that secure because it can be copied, forgotten or seen by someone. In biometrics use of distinctive biological (e.g., fingerprints, face, iris) and behavioral (e.g., speech) characteristics, called biometric identifiers, for automatic recognition of individuals are used. Hence, biometric systems offer a more appropriate solution to the problem of the user authentication system but the main concern with the biometric based authentication systems is to protect the template of a user which is generally stored in a database.

In general, template protection methods are designed to guarantee:

- Irreversibility: the impracticability to reconstruct the original template from the protected template.
- Diversity: the property to derive totally different protected templates from the original protected template
- Accuracy: the preservation of the recognition accuracy once the matching is carried out on protected templates
- Revocability: the probability to come up with a compromised template and reissue a new one based on the same biometric information.

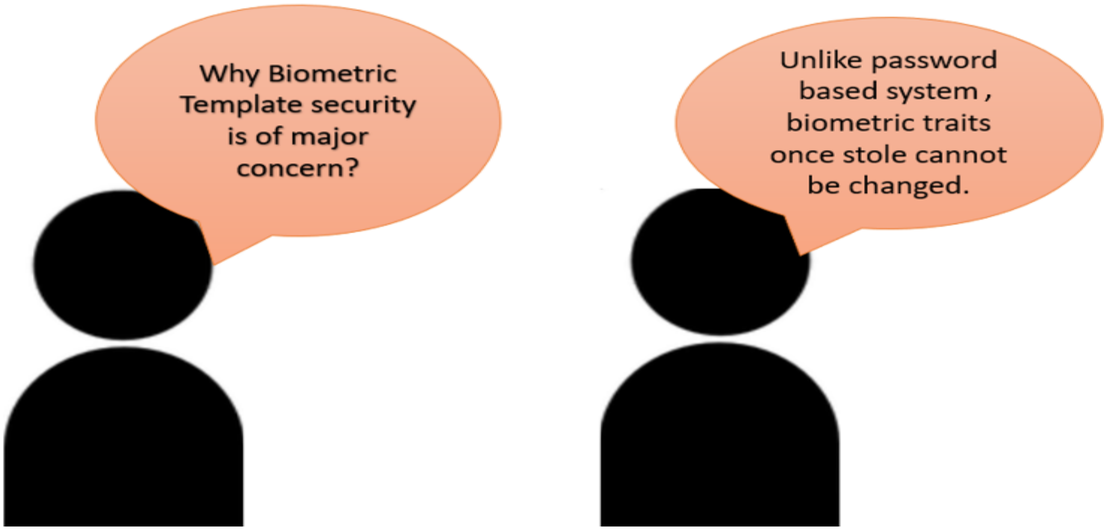
Why Biometric Template security is of major concern?
Unlike password based system , biometric traits once stole cannot be changed.

Figure 1.1: Importance of biometric template

Biometric cryptosystems can operate in one of the following three modes:

1. Key binding
2. Key release
3. Key generation

Systems working in key binding and key generation modes are most secured systems. But, due to large intra-class variations in biometric data such cryptosystems are difficult to implement. Factors like translation, nonlinear distortion, rotation, skin conditions, and noise result in intra-class variations in the fingerprints.
Fingerprint recognition is one of the most popular biometric techniques utilized in automatic personal identification and verification. Most fingerprint matching systems are based on four types of fingerprint representation schemes as shown in Figure:1.2:

- Grayscale image
- Phase image
- Skeleton image
- Minutiae

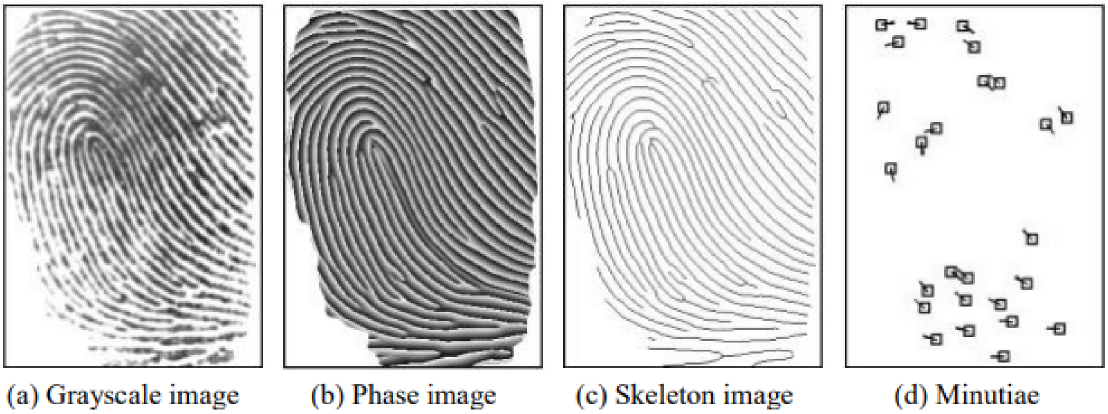

Figure 1.2: Fingerprint representation scheme [3]

The minutiae based representation has become the most widely used fingerprint representation technique. Minutiae constitute the two main local ridge characteristics as shown in Figure:1.3:

- Ridge ending: the point where a ridge ends abruptly.
- Ridge bifurcation: the point where a ridge forks or diverges into branch ridges.

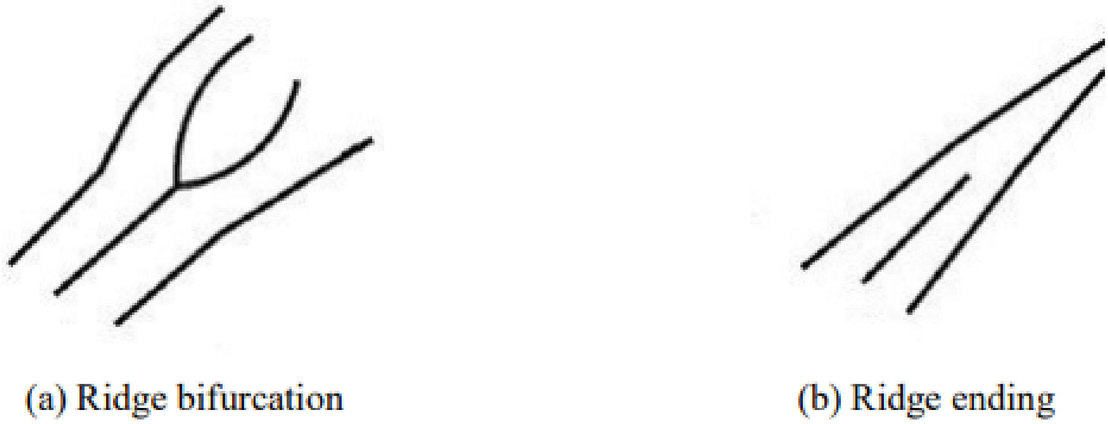

Figure 1.3: Commonly used miutiae types

Each of the ridge endings and ridge bifurcations types of minutiae has three attributes, namely, the x-coordinate, the y-coordinate, and the local ridge orientation θ as shown in Figure:1.4

Most of the issues with fingerprint based biometric systems are that they directly store fingerprint information in the form of a minutiae template. From the knowledge of these minutiae points, the original fingerprint can be reconstructed and

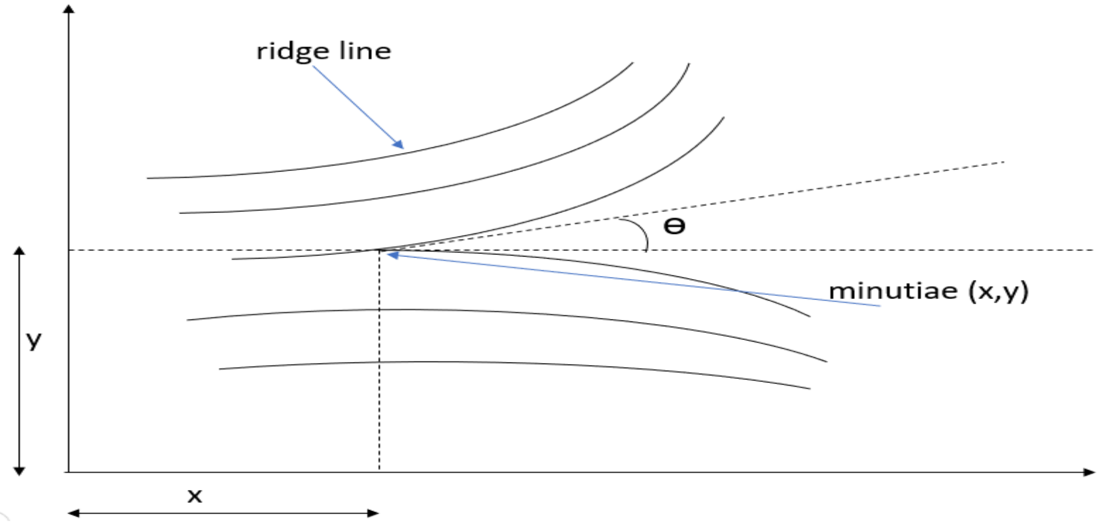

Figure 1.4: Minutiae attributes

the identity of the person is compromised. Juels and Sudan[1] proposed a cryptographic construction called a Fuzzy vault that operates within the key binding mode and can compensate for intra-class variations in the biometric data. In the Fuzzy vault, only the transformed version of the template is stored in the database rather than storing the original template with minutiae information. Thus, aligning the query fingerprint with the original template is a very challenging task. We have presented a Fuzzy vault scheme with different alignment and filtering techniques. We have used the PCA technique for alignment.

1.1 Motivation

With the increasing magnitude of identity fraud in our society, it is necessary to possess some reliable data secured system. By using stronger authentication schemes such as biometrics, limitations of password based authentication may be mitigated. Biometric systems identify a person based on biological or behavioral traits, like a fingerprint, face, voice, iris, etc. As these attributes are specific to a particular individual and such traits cannot be lost or forgotten, biometric based systems are much more authenticate than password based. Biometric cryptosystems provide a reliable solution to the problem of user authentication but the main problem with such systems is to secure the template stored in the database. Most of the biometric systems directly store the extracted features into the database.

As a result, if the biometric template gets leaked, then the original biometric attribute can be reconstructed from it and the identity of a person is compromised. In contrast to a stolen password or credit card, it is not possible for an authenticated user to revoke his/her biometric templates and replace them with another set of identifiers. Hence, the security of the biometric cryptosystems is of major concern. So, we have proposed a Fuzzy vault construct which not solely secures the secret key but also the biometric template.

1.2 Organization of the report

The remaining portion of the report is organized as follows. Literature Review is described in Chapter 2. Chapter 3 describes the proposed methodology in detail. The database used and the results of the work are discussed in Chapter 4. Finally, Chapter 5 draws the conclusions of this work and provides the future scope.

Chapter 2

Literature Review

In the biometrics community, the security and privacy of such systems are becoming a major concern[5]. In the literature, several methods have been proposed for implementing a biometric cryptosystem in key binding/generation modes. A detailed review of various biometric cryptosystems has been presented in [6]. A Fuzzy vault technique projected by Juels and Sudan [1] operates in the key binding mode and can compensate for intra-class variations in the biometric data. A key binding algorithm for an optical correlation-based fingerprint matching system was proposed by Soutar et al.[7]. In this algorithm, at the time of enrollment, a cryptographic key of length 128 bits is bind with the user's fingerprint image. Using the correlation filter functions a key is then retrieved only upon the successful authentication. Another system for template protection is proposed by Linnartz and Tuyls [8]. They encoded a secret S to generate the helper data W from an enrolled template X which they assumed is noise-free at the enrollment time. The biometric query Y which is a noisy version of X is then used to decrypt W to generate a the message which is just about identical as S.

Clancy et a1.[9] projected a fuzzy vault theme based on the location of minutia points in a fingerprint. An impractical assumption made by them was that the query and template image are prealigned. Further, 4 fingerprint impressions of a user were used for enrollment for identifying the reliable minutia points and without being actually implementing the error-correction step it was simulated. The FRR of their system was about 20–30%. Yang and Verbauwhede [10] also proposed a fingerprint-based fuzzy vault based solely on the location attributes of the minutia points. A reference minutia and the relative position of the remaining minutia points with regard to the reference minutia were depicted in the polar coordinate system and 4 fingerprint impressions were used during enrollment for the same. This theme was evaluated on a small database of 10 fingers and an FRR of about 17% was reported. A geometric hashing technique proposed by Chung et al. [11] is used to perform alignment in a fuzzy vault based on fingerprint minutiae points. [4] introduced a modification to the fuzzy vault scheme, that eliminated the requirement for Reed–Solomon polynomial decoding. They additionally projected the use of helper data to mechanically align the template and query minutiae sets. Our fuzzy vault implementation mainly extends the ideas presented in [2]. Fingerprint alignment is the most difficult task within the biometric systems and we have used the PCA technique for it.

Chapter 3

Proposed Method

The projected fuzzy vault scheme is based on the minutiae points. It is represented in Figure:3.1. We have considered the ridge endings and bifurcations type minutiae as shown in Figure:1.3, and the location attribute(x,y) of the minutiae point as shown in Figure:1.4 for implementation of the Fuzzy vault construct.
We have implemented the Fuzzy vault construct as proposed in [2] with significant modifications. In this technique, several sets are generated from the unlocking set and polynomial are recreated using Lagrange Interpolation. The CRC-based error detection technique is used to identify the correctness of the polynomial generated and the secret key is revealed as output if no error generated.

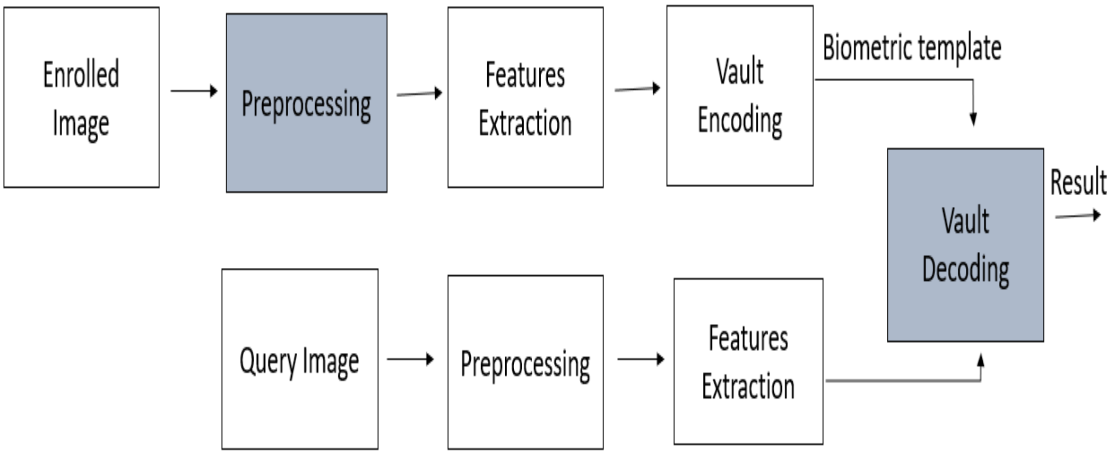

Figure 3.1: Flow chart of the proposed fuzzy vault technique with main modifications in the highlighted part

Our implementation differs from the implementation proposed in [2] in the following aspects:

- We are using only the location attributes (i.e x and y coordinates) of a minutia point in our implementation whereas they are also considering the orientation attribute θ.
- Fingerprint alignment is the most challenging part of the fingerprint matching system. We are using PCA for the alignment of the query image to the template image whereas they have proposed the helper data-based method for alignment.
- Relative distance minutiae matching algorithm is used which is described in Section 3.5.

3.1 Preprocessing

Minutiae extraction algorithm is performed after applying the following preprocessing steps as shown in Figure:3.2 on the original image :

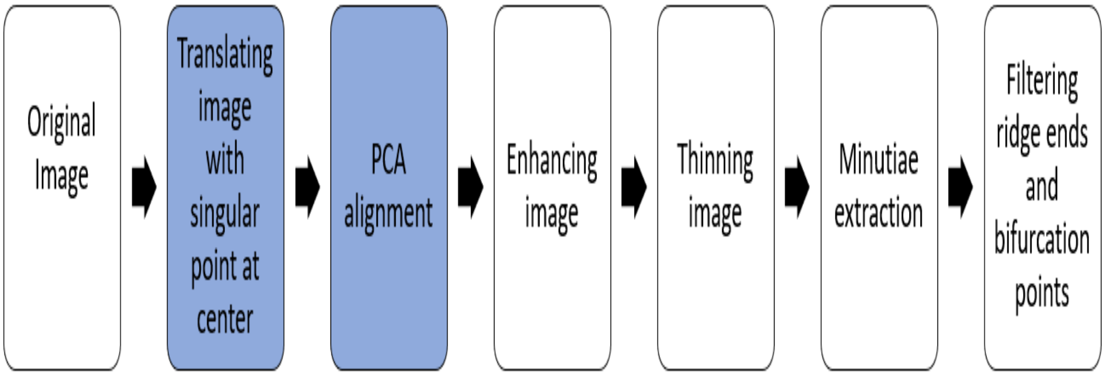
Original Image
Translating image with singular point at center
PCA alignment
Enhancing image
Thinning image
Minutiae extraction
Filtering ridge ends and bifurcation points

Figure 3.2: Flow chart for preprocessing steps and minutiae extraction

1. Image Translation: Singular point in the original image is determined and the whole image is translated such that a singular point occupies the center of the image.
2. Image Alignment: PCA alignment is performed on it to nullify the rotational distortion.

3. Enhancing: Improvement of fingerprint image quality is projected with the Gabor Filter methodology. The steps taken begin by increasing the native image contrast by applying the AHE methodology, then, corrected by the Gabor Filter and binarization strategies.

4. Thinning: Thinning is a morphological operation that is used to eliminate selected forefront pixels from binary images. It can be used for many applications but especially helpful for skeletonization. During this mode it neatens up the output of edge detectors by reducing all lines to single-pixel thickness. Thinning is generally applied to binary images, and produces another binary image as output.

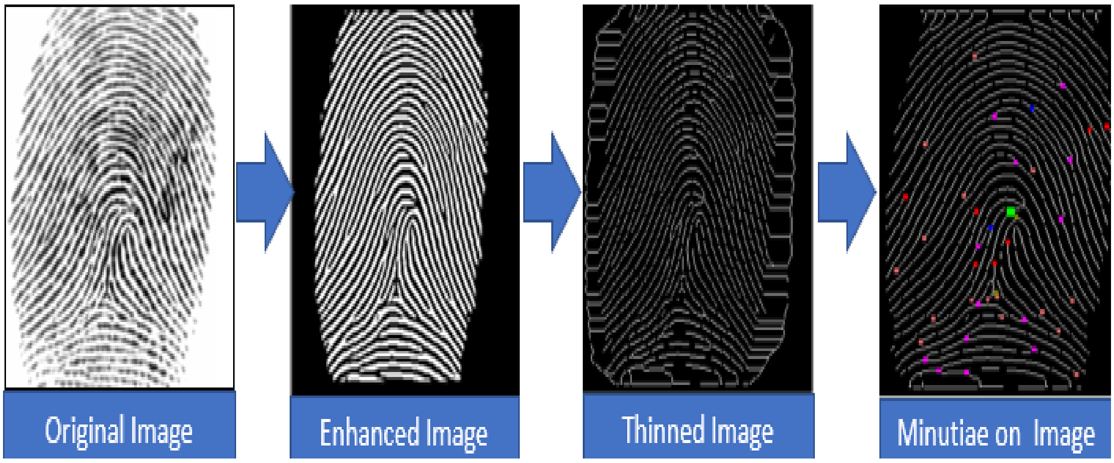

Figure 3.3: Minutiae extraction steps

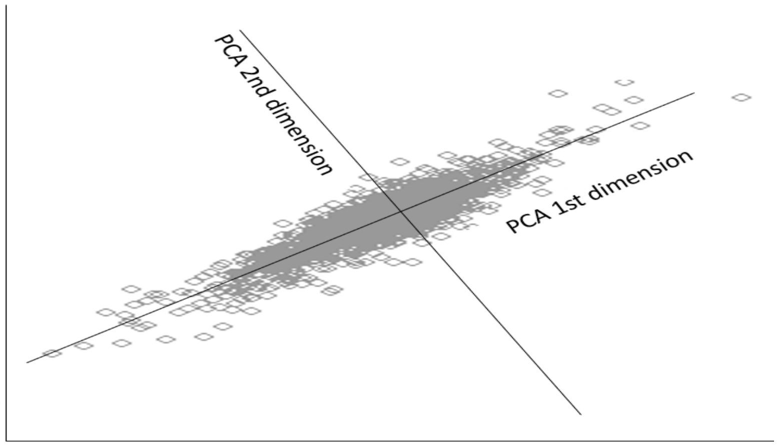

Figure 3.4: Orthogonal vectors representing PC1 and PC2 on a given dataset

3.2 Principal Component Analysis (PCA)

The alignment of a query fingerprint image with the enrolled fingerprint image is a very challenging task. From the orientation field of the fingerprint template high curvature points are obtained and stored as helper data to help in alignment. This is the most common technique used for alignment of fingerprints. We have proposed a new alignment technique based on PCA method.

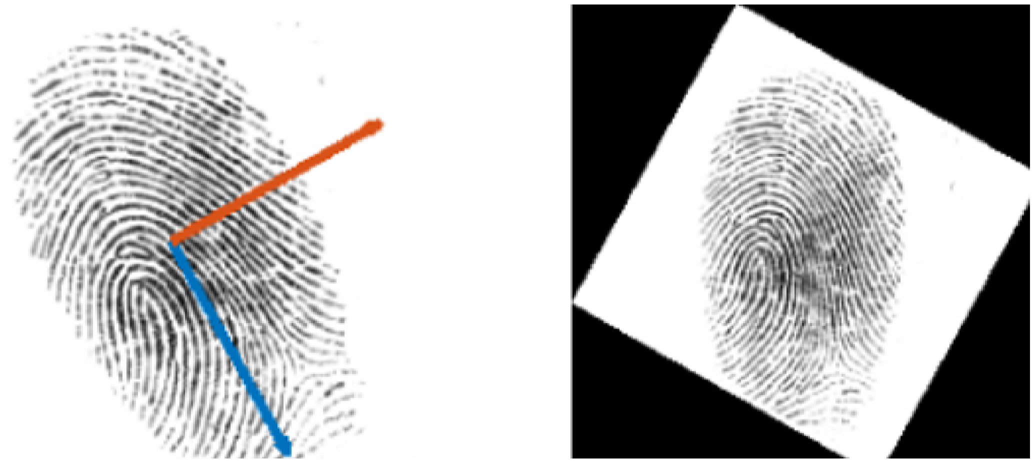

Figure 3.5: PCA applied on the left aligned image

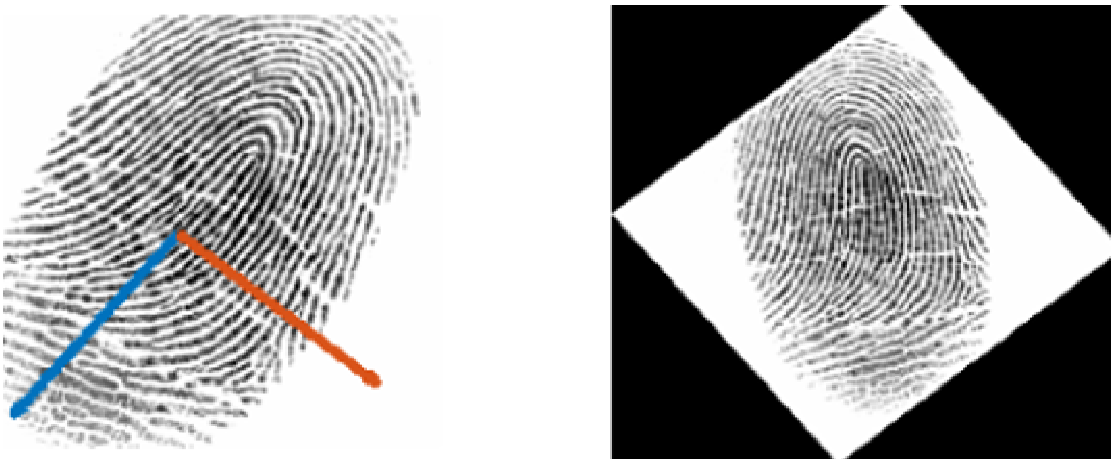

Figure 3.6: PCA applied on the right aligned image

PCA is a technique that uses an orthogonal transformation to convert a group of observations of possibly correlated variables into a set of values of linearly unrelated variables known as principal components.

This transformation is outlined in a manner that the first principal component has the largest possible variance and each succeeding component, in turn, has

the highest variance possible under the constraint that it is orthogonal to the preceding components.
The resulting vectors (each being a linear combination of the variables and containing n observations) are an uncorrelated orthogonal basis set. PCA is sensitive to the relative scaling of the initial variables.

3.3 Vault Encoding

The Vault is encoded as follows:

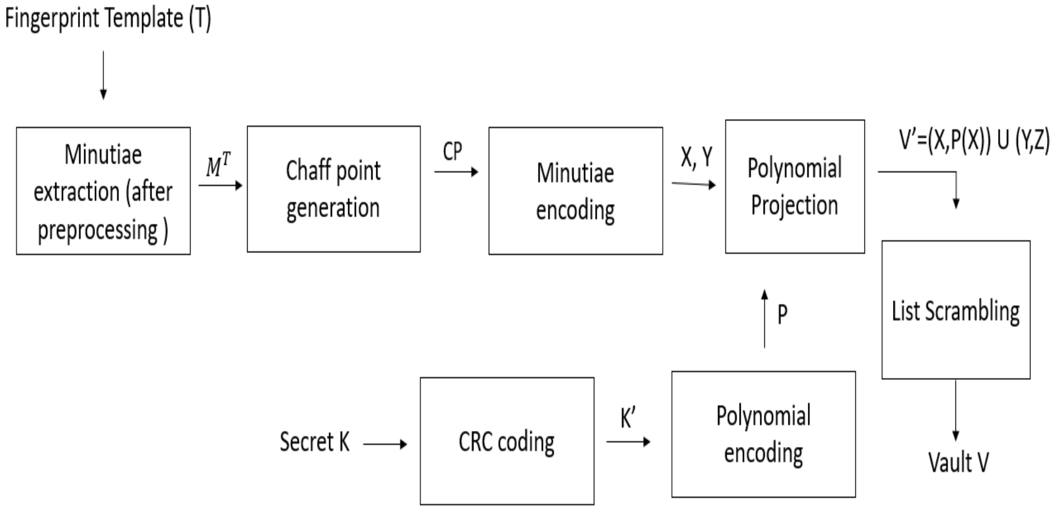

Figure 3.7: Flow chart for the vault encoding

1. From the given template fingerprint image T, after applying the steps mentioned in Figure:3.2 on the image template, minutiae set $M^T = (m_i^T)_{i=1}^N$ is obtained, where N is the number of minutiae in T.

2. Only r well separated minutiae are chosen i.e. the minimum distance between any two selected minutiae must be greater than a certain threshold value δ_1 and forms selected minutiae set SM^T. Distance between two points (x_1, y_1) ans (x_2, y_2) is calculated by:

$$D = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \tag{3.1}$$

3. The chaff point set $CP = (m_k)_{k=1}^s$ is then generated as follows. A chaff point $c = (x, y)$ whose minimum distance from all the points in SM^T is greater

than δ_1 is added to the set.

4. The minutia attributes (x, y) is quantized and each is represented as a bit string of length 8 represented by B_x and B_y respectively. Then a 16 bit number is obtained by appending the bit strings B_x and B_y. After that a decimal number corresponding to 16 bit is obtained. Using this method both selected minutiae set (SM^T) and chaff point set (CP) are encoded. Encoded values of selected template minutiae and chaff points are represented by $X = (x_j)_{j=1}^{r}$ and $Y = (y_k)_{k=1}^{s}$ respectively.

5. A secret of length $16n$ bits, where n is the degree of the encoding polynomial, can be easily secured by our method. A new secret K' of length $16(n+1)$ bits is obtained by appending a 16 bit CRC code to a secret K. For generating the CRC bits generating polynomial used is

$$G = x^{16} + x^{15} + x^2 + 1 \tag{3.2}$$

6. A polynomial P of degree n is encoded by a secret K' by partitioning it into $(n+1)$ 16 bit values $c_0, c_1, c_2...., c_n$ and considering them as coefficients of P i.e.

$$P = c_n x^n + ... + c_0 \tag{3.3}$$

7. A set $P(X) = \{P(x_j)\}_{j=1}^{j=r}$ is obtained by evaluating the polynomial P on all the points in the selected minutiae set X. Then the corresponding elements of the sets X and $P(X)$ form the locking set $L = \{x_j, P(x_j)\}_{j=1}^{r}$. By selecting values randomly such that the points (y_k, z_k) do not lie on the polynomial P, set $Z = \{z_k\}_{k=1}^{s}$ is obtained. The chaff points set is represented by $C = (y_k, z_k)_{k=1}^{s}$. The union of chaff set C and locking set L is represented by V'.

8. Vault V represented as $V = (a_i, b_i)_{i=1}^{t}$, where $t = r + s$, is obtained by shuffling the elements of V'. Only the vault is stored in the database, unlike vault and helper data as proposed in [2].

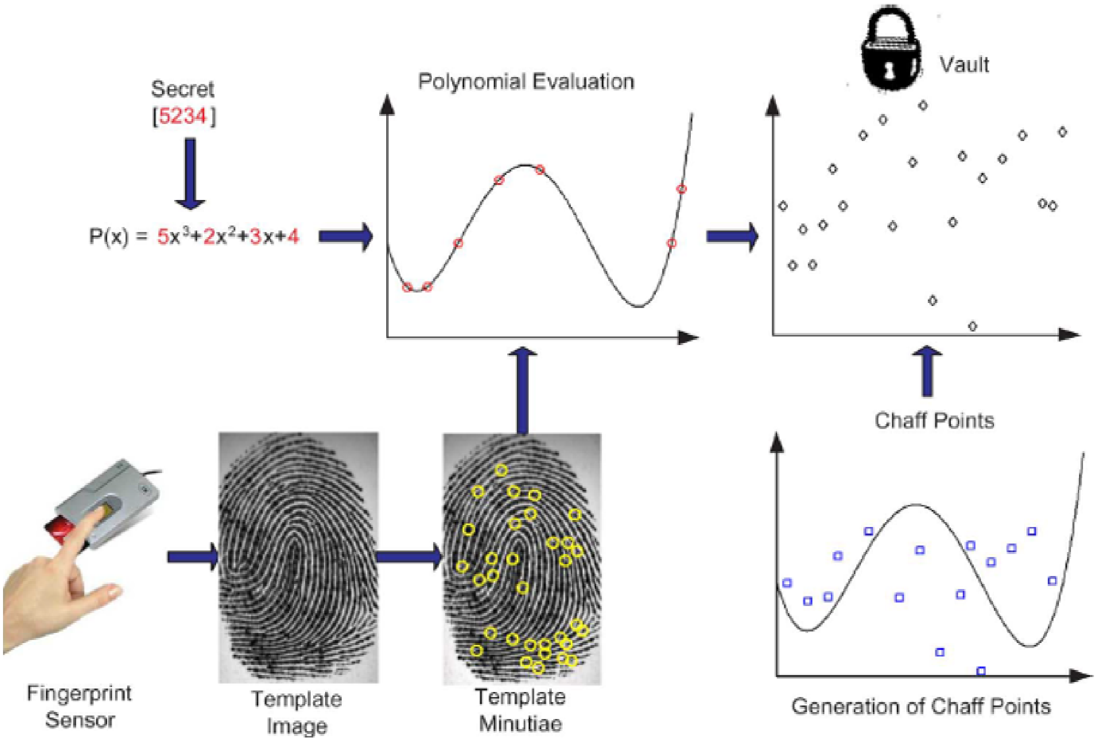

Figure 3.8: Vault encoding [2]

3.4 Vault Decoding

The process of decoding the vault consists as follows:

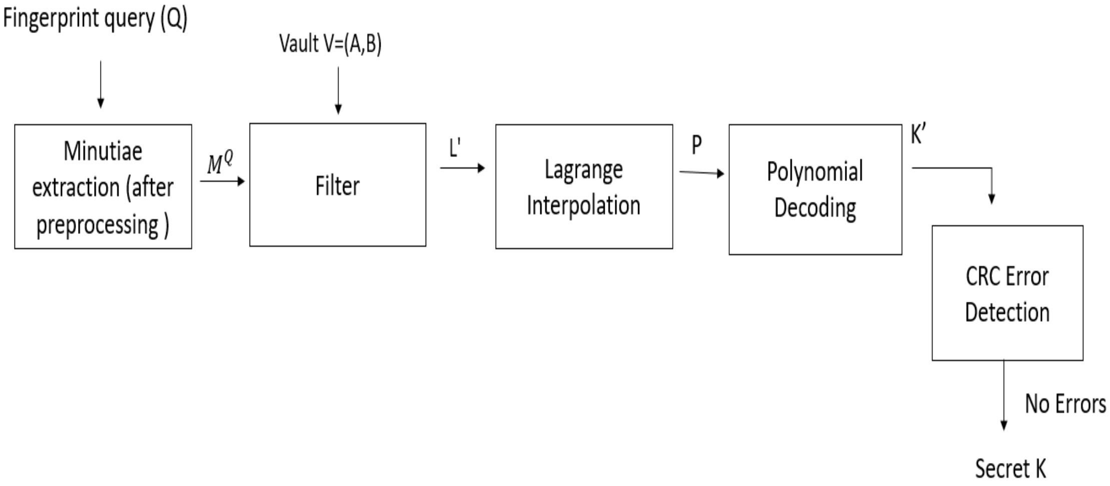

Figure 3.9: Flow chart for the vault decoding

1. From the given query fingerprint image Q, we obtain the query minutiae set $M^Q = (m_i^Q)_{i=1}^N$ after applying the steps described in Figure:3.2.

2. Only r well separated minutiae are chosen i.e. the minimum distance between any two selected minutiae is greater than a threshold δ_1. The selected minutiae set is thus represented by $SM^Q = (m_j^Q)_{j=1}^r$.

3. The query minutiae set M^Q is used to filter the chaff points in the vault as follows. The x coordinate values of the points in the vault (i.e., $A = (a_i)_{i=1}^t$) are first represented as bit strings of length 16. The 16 bit strings then are partitioned into two strings of length 8 bits B_x and B_y respectively. These are then converted into quantized minutia attribute values x and y. Hence, we obtain the set $M^V = \{m_i^V\}_{i=1}^s$.

4. If the minimum distance between the point $m_i^V \in M^V$ and all of the selected minutiae in the query $m_j^Q \in SM^Q$ is greater than a threshold δ_2 then the ith element of the set M^V is marked as a chaff point. This is a coarse filtering step and it filters out a significant number of the chaff points. Let $SM^V = (m_k)_{k=1}^N$ be a subset of M^V consist of only those points that are not marked as chaff.

5. Relative distance minutiae matching algorithm described in Section[3.5] is then applied which further removes the chaff point. Only those points which have a corresponding minutia in SM^Q and that are contained in SM^V are added to the unlocking set L' represented by $L' = (a, b)_{i=1}^{r'}$. Each query minutiae can have no more than one corresponding minutia in SM^V, thus we have $0 <= r' <= r$, where r is the size of the selected query minutiae set.

6. $(n + 1)$ unique points are necessary to find the coefficients of a polynomial of degree n. Authentication failure occurs when $r' < (n + 1)$. Otherwise, we consider all possible subsets L" of size $(n+1)$ of the unlocking set L' and by using Lagrange interpolation method we construct a polynomial P' for each subset. If $L" = (a_i, b_i)_{i=0}^n$ is a specific candidate set, P' is obtained as

$$P'(x) = \frac{(x - a_1)(x - a_2)...(x - a_n)}{(a_0 - a_1)(a_0 - a_2)...(a_0 - a_n)} b1 + ... \frac{(x - a_0)(x - a_1)(x - a_2)...(x - a_{n-1})}{(a_n - a_0)(a_n - a_1)...(a_n - a_{n-1})} \tag{3.4}$$

Then the polynomial formed is given by

$$P'(x) = c'_n x_n + c'_{n-1} x_{n-1} + ... + c'_0 \tag{3.5}$$

7. The coefficients $c'_0, c'_1, ...c'_n$ of the polynomial P' obtained are 16 bit values which are concatenated to obtain a string K" of length $16(n+1)$ bits. Error detection code CRC is then applied to K" to identify the correctness of the polynomial generated. If an error is generated then it indicates that an incorrect secret has been decoded and again the same method is repeated for the next candidate set L". If no error is generated, it indicates with a very high probability that $K" = K'$ and the 16 bit CRC code is removed from K' and the system reveals the secret K.

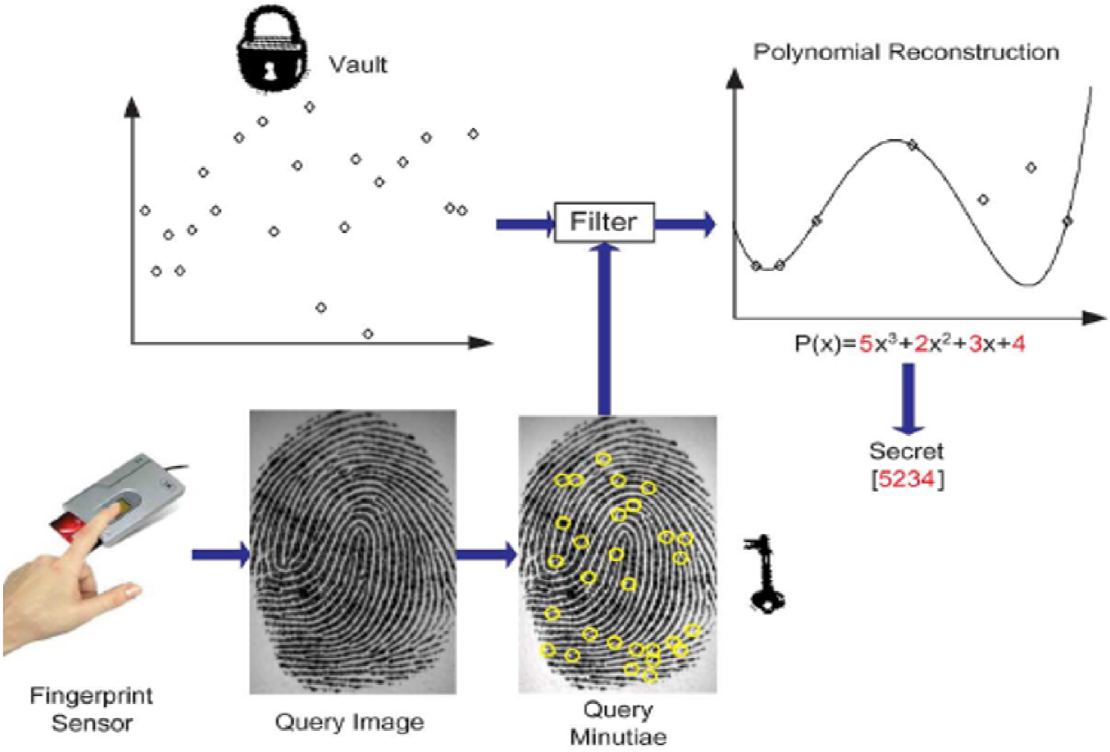

Figure 3.10: Vault decoding [2]

3.5 Vault Filtering

It includes coarse filtering and relative distance minutiae matching:

3.5.1 Coarse filtering

A point from the vault is added to set A only if the distance of vault point from any of the query minutiae points lies within certain threshold value δ_2. This step removed 80% chaff points from the vault.

3.5.2 Relative distance minutiae matching

Set A is further filtered to obtain the more genuine points. The filtered points then form the unlocking set.
For every query minutiae, a point is chosen from set A which meets the following two conditions:

1. Distance between query minutiae and chosen vault point is less than the threshold value, δ_2.

2. Distance of both query minutiae point and chosen vault point from singular point must be the same because the relative distance does not vary due to translational and rotational effect. But for calculation purposes, relative difference of δ_3 is considered.

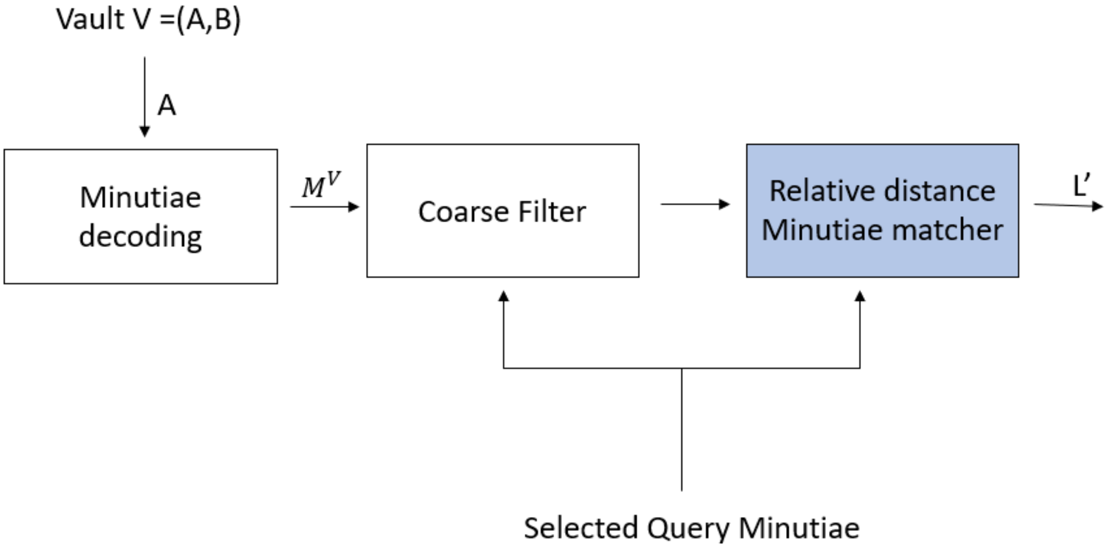

Figure 3.11: Flow chart for Vault Filtering

Chapter 4

Results and Discussion

The performance of the proposed Fuzzy vault implementation is evaluated on FVC2002-DB1 and FVC2002-DB2 fingerprint databases. The characteristics of these two databases are summarized in Table:4.1.
FVC2002 database is a public domain database for fingerprint images. It consist of four different databases (DB1, DB2, DB3 and DB4) which were collected by using the following different sensors/technologies. Sample image of each dataset of FVC2002 database is shown in Figure:4.1. Each database consist of impressions from 100 users(u) and each user has enrolled 8 impressions per finger(f).

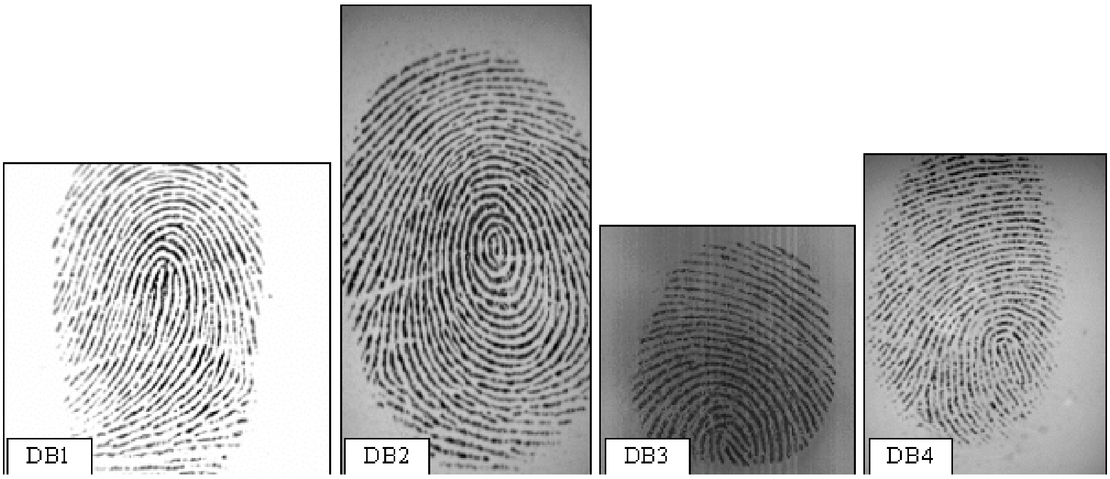

Figure 4.1: Sample image of each dataset of FVC2002 database

We have performed our experiment on FVC2002 DB1 and FVC2002 DB2 databases only. 3, 4, 5, and 6 impression numbers in FVC2002 database is formed by exaggerated displacement and rotation, thus we have not taken these images into consideration. It is assumed that users in a biometric cryptosystem will provide good quality biometric data in order to get back their cryptographic keys. Thus, 1, 2, 7, and 8 impression number are used for experimentation.

Parameters	**DB1**	**DB2**	**DB3**	**DB4**
(u X f)	100 X 8	100 X 8	100 X 8	100 X 8
Sensor Type	Optical Sensor	Optical Sensor	Capacitive Sensor	SFinGe v2.51
Image Size	388 X 374	296 X 560	300 x 300	288 X 384
Resolution	500 dpi	569 dpi	500dpi	500dpi

Table 4.1: Comparison of different datasets of FVC2002 database

We have considered the following two scenarios for the fuzzy vault implementation:-

- One impression each for encoding and decoding.
- Two impressions for encoding and one impression for decoding the vault.

Parameters used	
No. of authentic points within the vault, r	18-30
Encoding polynomial degree, n	8-10
Total no. of points within the vault, t	218-230
Total no. of chaff points in the vault, s	200
Minimum distance between minutiae and chaff point, δ_1	26
Maximum distance between point selected by coarse filtering and query minutiae, δ_2	12
Absolute relative difference from the singular point, δ_3	6

Table 4.2: Parameters used for the implementation of a fuzzy vault

The parameters utilized in our implementation is listed in Table:4.2. Length of the secret key to be secured ultimately decides the degree of a polynomial used for encoding the vault. A polynomial of degree n can secure the the secret of length 16n bits. For decoding a polynomial of degree n, $(n+1)$ authentic minutiae points are required. The number of genuine points in the vault are r and about 10 times of the genuine points are added to the vault as chaff points $(s = r + t)$. Minutiae attributes x and y are encoded by using 8 bits each.

For the given database the parameters mentioned in Table:4.2 are the optimal choice.

The norm used for evaluating the performance of the proposed system are the GAR and FAR. The GAR is defined as a percentage of authentic users accepted by the system. It is given by GAR=100-FRR. FAR is the measure of the probability that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

The results in Table:4.3 and Table:4.4 are performed on FVC2002-DB1 database, and results in Table:4.5 and Table:4.6 are performed on FVC2002-DB2 under different scenarios.

SCENARIO	**N=8**		**N=10**	
	GAR%	FAR%	GAR%	FAR%
One Template, One Query	93%	0.04%	89%	0.02%

Table 4.3: GAR and FAR obtained on degree 8 and degree 10 polynomials

One Template , One Query means one image is used for encoding and one image for decoding. The results obtained in Table:4.3 is performed both for degree 8 and degree 10 polynomials. For GAR calculation, the number of genuine attempts are 100 as vault is constructed by using impression 1 and decoded by impression 2 for each user.

Impostor attempts were attempted by trying to decode a user's vault using impressions from all of the other users. Hence, the number of impostor attempts is 4950.

When the polynomial of degree 8 is used than 93 out of 100 genuine attempts were successful. When the polynomial of degree 10 is used than GAR decreases to 89% because the number of genuine minutiae matching point required for polynomial decoding increases.

SCENARIO	**N=8**	
	GAR%	FAR%
One Template, One Query	80.6%	0.04%

Table 4.4: GAR and FAR obtained on degree 8 polynomial on whole dataset of FVC2002 DB1

These results in Table:4.4 are obtained by performing the experiment on the whole dataset. For GAR total number of genuine attempts are 2800. For each user 8 fingerprints are available out of which any one can be used for encoding and decoding. So, total number of ${}^{8}C_{2} = 28$ attempts are performed per user and thus 2800 attempts in total for 100 users. GAR observed is 80.6% as dataset also contain the poor quality images with exaggerated rotation and displacement.

SCENARIO	**Proposed method**		**Nandakumar et al.[2]**	
	GAR%	FAR%	GAR%	FAR%
One Template, One Query	89%	0.02%	91%	0.01%
Mosaiced Template, One Query	93.82%	0.03%	94%	0.02%

Table 4.5: Comparison of results obtained in [2] with the proposed method on degree 8 polynomial

The experiment results in Table:4.5 is performed on the FVC2002-DB2 dataset. Most of the research papers have performed their experiment on this dataset. So, we have compared the results of our experiment with the [2]. The experiment is performed under two scenarios.

- One Template, One Query: GAR and FAR obtained is 89% and 0.02% respectively, which is comparable to what proposed in [2].
- Mosaiced Template, One Query: Two images are used for encoding and one for decoding. The GAR increases to 93.82% from 89%. Hence, by enrolling multiple images accuracy of the system can be improved.

SCENARIO	**Proposed method**		**Nandakumar et al.** [2]		**Uludag et al.** [4]	
	GAR%	FAR%	GAR%	FAR%	GAR%	FAR%
One Template, One Query	89%	0.02%	91%	0.01%	79%	0%
Mean decoding time on 3.4GHz processor	7.33 s		8 s		52 s	
Storage space required for	vault		vault and helper data		vault and helper data	

Table 4.6: Comparison of results obtained in [2] and [4] with the proposed method on degree 8 polynomial

The experiment results in Table:4.6 is performed on the FVC2002-DB2 dataset. The results obtained are compared with the results in [2] and [4]. Our accuracy is better than the system proposed in [4], but less than the one proposed in [2]. In terms of mean decoding time and storage space required, our system is better than both.

Chapter 5

Conclusions and Future Work

5.1 Conclusions

Since biometric traits are associated forever with a user, they cannot be modified. If biometric data is compromised then the identity of a person is lost forever. In government and commercial applications, such systems are being deployed in large numbers. Thus, the security and privacy of biometric systems are gaining global attention. Among the various issues, protecting the biometric template is a major concern. Biometric cryptosystems are projected to extend the associated security as they store the transformed versions of the templates instead of storing the original version of the template. An instance of such systems is the fuzzy vault construct.

We have shown the results of a fuzzy vault construct using minutiae points. The vault performs with reasonable accuracy. AES Key of length 128 bits can be easily secured using the projected technique. We have made use of a PCA technique to align the template and the query image appropriately. The proposed alignment achieves reasonable accuracy without using any storage space as compared to earlier proposed techniques used for alignment. The GAR(89%) and FAR(0.02%) obtained are comparable to the results mentioned in [2], and are better than what mentioned in [4]. In terms of mean decoding time and storage space required, our system is better than both. Moreover, our technique is much simpler to implement.

5.2 Future Work

- Cancellable biometrics can be combined to make the proposed technique more robust.

- As we have observed that using two images for encoding the GAR of the system is increased. Hence, multiple images can be used for enrollment to increase the genuine acceptance rate.

- Additional attributes such as orientation, ridge curvature, ridge counts, etc. can be incorporated into the current system apart from location attribute (x,y) to achieve higher recognition rates.

Bibliography

[1] A Juels and M Sudan. A fuzzy vault scheme. in proc. ieee int. In *Symp. Inf. Theory, Switzerland*, page 408, 2002.

[2] Karthik Nandakumar, Anil K Jain, and Sharath Pankanti. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE transactions on information forensics and security*, 2(4):744–757, 2007.

[3] Jianjiang Feng and Anil K Jain. Fingerprint reconstruction: from minutiae to phase. *IEEE transactions on pattern analysis and machine intelligence*, 33(2):209–223, 2010.

[4] Umut Uludag, Sharath Pankanti, and Anil K Jain. Fuzzy vault for fingerprints. In *proceedings of International Conference on Audio-and Video-Based Biometric Person Authentication*, pages 310–319. Springer, 2005.

[5] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. Multimodal biometric systems. *Handbook of fingerprint recognition*, pages 233–255, 2003.

[6] Gregory C Sharp, Sang W Lee, and David K Wehe. ICP registration using invariant features. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(1):90–102, 2002.

[7] Zümrüt Müftüoğlu and Tülay Yildirim. Comparative analysis of crypto systems using biometric key. *Procedia Computer Science*, 154:327–331, 2019.

[8] Jean-Paul Linnartz and Pim Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In *proceedings of International Conference on Audio-and Video-Based Biometric Person Authentication*, pages 393–402. Springer, 2003.

[9] T Charles Clancy, Negar Kiyavash, and Dennis J Lin. Secure smartcardbased fingerprint authentication. In *proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, pages 45–52. ACM, 2003.

[10] Shenglin Yang and Ingrid Verbauwhede. Automatic secure fingerprint verification system based on fuzzy vault scheme. In *Proceedings.(ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.*, volume 5, pages v–609. IEEE, 2005.

[11] Yongwha Chung, Daesung Moon, Sungju Lee, Seunghwan Jung, Taehae Kim, and Dosung Ahn. Automatic alignment of fingerprint features for fuzzy fingerprint vault. In *proceedings of International Conference on Information Security and Cryptology*, pages 358–369. Springer, 2005.