

Master Thesis
Electrical Engineering
September 2018



Combination of Fingerprints for New Identity and Protection

Mucharla Harindra Sai Tej
Raj Sekhar Sana
Satyanarayana Namuduri

Department of Applied Signal Processing
Blekinge Institute of Technology
SE-371 79 Karlskrona, Sweden

This thesis is submitted to the Department of Applied Signal Processing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Electrical Engineering with emphasis in Signal Processing.

Contact Information:

Author(s):

Mucharla Harindra Sai Tej

E-mail: harindra.saitej@gmail.com.

Raj Sekhar Sana

E-mail: rajsekhsana@gmail.com.

Satyanarayana Namuduri

E-mail: satya.namuduri21@gmail.com

Thesis Supervisor:

Dr. Josef Ström Bartunek

Dept. Applied Signal Processing

E-mail: josef.strombartunek@bth.se

University Examiner:

Dr. Sven Johansson

Dept. Applied Signal Processing

E-mail: sven.johansson@bth.se

Dept. Applied Signal Processing
Blekinge Institute of Technology
SE-371 79 Karlskrona, Sweden

Internet : www.bth.se
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

Abstract

We propose here a novel framework for ensuring unique mark security by joining two distinct fingerprints into another personality. In the enlistment, two fingerprints are caught from two diverse fingers. We extricate the details positions from fingerprints and the reference focuses from the two fingerprints. In view of this removed data and our proposed coding procedures, a joined detail layout is produced and put away in a database. In the validation, the framework requires two query fingerprints from a similar two fingers which are utilized as a part of the enlistment. A two-organize unique mark coordinating procedure is proposed for coordinating the two inquiry fingerprints against a consolidated particulars format. By putting away the joined details format, the total particulars highlight of a solitary unique mark won't be traded off when the database is stolen. Besides, in view of the likeness in topology, it is troublesome for the aggressor to recognize a joined details format from the first particulars layouts. With the assistance of a current approach, we can change over the consolidated particulars layout into a genuine clone joined unique finger impression. Along these lines, another virtual personality is made for the two unique fingerprints, which can be coordinated utilizing details based unique mark coordinating calculations. The trial comes about demonstrate that our framework can accomplish a low error rate. Contrasted and the best in class strategy, our work has the favorable position in making a superior new virtual character when the two distinct fingerprints are arbitrarily picked.

Keywords: Combination, fingerprint, minutiae, protection, Privacy, Databases, Authentication, Fingerprint recognition.

Acknowledgment

Firstly, we would like to express my sincere gratitude to our supervisor Dr. Josef Ström Bartůněk for the continuous support of our master thesis study and related research, for his patience, support, and immense knowledge. His guidance helped us during research and writing of this thesis. We could not have imagined having a better advisor and mentor for our thesis study.

Finally, a big thanks to our family and friends who supported us during the entire time of study.

Contents

Abstract	i
1 Introduction	1
1.1 Motivation	1
1.2 Problem Statement	1
1.3 Problem Solution	1
1.4 Aim and Objectives	2
1.5 Research Questions	2
1.6 Outline of Thesis	2
2 Literature Study	4
3 Background	7
3.1 Fingerprint History	7
3.2 Fingerprint Pattern	7
3.3 Fingerprint Sensing	9
3.4 Fingerprint Database	10
3.5 Fingerprint Recognition	11
4 Proposed Method	13
4.1 Overview	13
4.2 Preprocessing	14
4.2.1 Histogram Equalization	14
4.2.2 Binarization	16
4.2.3 Thinning	16
4.3 Rotation of fingerprint	17
4.3.1 Masking	17
4.3.2 Eigen Values and Eigen Vectors	18
4.4 Feature Extraction	21
4.4.1 Minutiae Detection and Extraction	22
4.4.2 Location and Orientation of Minutiae Positions	24
4.5 Post Processing	25
4.5 Combination and Shifting axes	26
4.6 Fingerprint Matching	30
5 Performance Evaluation	31
5.1 Biometric Classification	31
5.2 Performance Evaluation Factors	31
5.2.1 False Acceptance Rate (FAR)	31
5.2.2 False Rejection Rate (FRR)	32
5.2.3 Equal Error Rate (EER)	32

6 Results and Discussion	34
6.1 Results	34
6.1.1 Genuine Scores	34
6.1.2 Imposter Scores	34
6.2 Discussion	40
6.2.1 Answers to Research Questions	40
6.2.2 Problems faced during Implementation	40
7 Conclusion and Future Work	42
7.1 Conclusion	42
7.2 Future Work	43
References	44

List of Figures

- Fig. 3.1. Fingerprint characteristics.
- Fig. 3.2 Fingerprint Patterns
- Fig. 3.3 Fingerprint Ridge Characteristics
- Fig. 3.4 Fingerprint acquired (a) is a latent one and another one (b) which is from the electronic sensing system.
- Fig. 3.5 Sample Images from each Data Base
- Fig. 3.6 Main modules of a fingerprint verification system.
- Fig. 4.1. Overview of proposed method
- Fig. 4.2. Technique to perform histogram equalization
- Fig. 4.3. Enhanced Image
- Fig. 4.4. Thinned Image
- Fig. 4.5. Fingerprints obtained in real time
- Fig. 4.6. Histogram of Fingerprint Image
- Fig. 4.7. Binary Mask of fingerprint image
- Fig. 4.8. Quadrants with phase angles
- Fig. 4.9. Fingerprint mask with imaginary eigen vectors
- Fig. 4.10. Rotated fingerprint mask
- Fig. 4.11. Rotated Fingerprint center
- Fig. 4.12. Flowchart of steps followed in minutiae detection
- Fig. 4.13. Pixel patterns for the detection of minutiae.
- Fig. 4.14. Detected Minutiae points
- Fig. 4.15. Minutiae orientation
- Fig. 4.16. Minutiae distribution of fingerprint 1
- Fig. 4.17. Minutiae distribution of fingerprint 2
- Fig. 4.18. Minutiae distribution of both fingers after shifting center and 50% used for combination
- Fig. 4.19. Minutiae distribution of combined fingerprint
- Fig. 5.1. Sample Curve indicating EER
- Fig. 5.2. Sample ROC Curve
- Fig. 6.1. Genuine Scores
- Fig. 6.2. Imposter Scores
- Fig. 6.3. FMR, FNMR, EER Curve

List of Tables

- TABLE I. Sensors and respective Image Data.
TABLE II. Genuine scores for combined fingerprint Vs Individual fingerprint.
TABLE III. Imposter scores of combined fingerprints 1 & 2 Vs other Individual fingerprint.
TABLE IV. Imposter scores of combined fingerprints 3 & 5 Vs other Individual fingerprint.
TABLE V. Imposter scores of combined fingerprints 4 & 6 Vs other Individual fingerprint.
TABLE VI. Imposter scores of combined fingerprints 7 & 8 Vs other Individual fingerprint.
TABLE VII. Imposter scores of combined fingerprints 9 & 10 Vs other Individual fingerprint.

List of Abbreviations

NBIS – NIST Biometric Image Software
NIST – National Institute of Standards and Technology
FVC – Fingerprint Verification Contest
CLAHE - Contrast Limited Adaptive Histogram Equalization
FMR – False Match Rate
FMNR – False Non- Match Rate
EER – Equal Error Rate
MINCDT – Minutiae Capture and Detection

1.1 Motivation

Fingerprints are most widely used biometric attributes in pin-pointing tasks and authenticity of systems. Every individual has exceptional fingerprints[1]. Now a days Fingerprint validation is utilized as a part of enormous sum and thief utilizes diverse procedures to track the unique mark confirmation. Encryption of the unique finger impression isn't adequate for the security assurance since unscrambling demonstrates the unique mark to the assailant. Henceforth, two unique fingerprints are joined into another unique finger impression to secure the protection of the finger impression[2]. Along these lines, it is changed into another personality. We will assess how the proposed calculation is better when contrasted with the current techniques where single fingerprints are utilized.

1.2 Problem Statement

In the advanced electronically brought together society, a profoundly predictable and dependable programmed individual verification strategy is required. The extremely renowned strategy which can be utilized effortlessly and which satisfies high security requirements is biometrics. Because of its outrageous uniqueness and changelessness, "finger impression" is the most generally utilized biometric system. To think about two unique mark pictures, an arrangement of perceiving and invariant highlights must be separated. The most segregating and delicate highlights are particulars focuses. That is a well-established actuality. Coordinating are so far thought to be a method which gives a high level of security in the majority of the unique finger impression confirmation frameworks.

Fingerprint security has become a challenge in the world. Suppose if the database containing fingerprints is stolen then there is a chance for the unauthorized persons to misuse and access. The main aim of this project is to develop a mixed fingerprint template which resembles as a single fingerprint and match it with fingerprints and calculate the similarity scores.

1.3 Problem Solution

With a specific end goal to build up a blended unique finger impression format we have taken two fingerprints from the Database and extricated the details focuses. Then by veiling the unique mark we found the focal point of the unique finger impression and moved to the source. We figured the eigen esteems for the unique finger impression through which angle is ascertained and pivoted the fingerprint (made it vertical). At that point, we consolidated the unique mark and put

away in Database. We contrast the question fingerprints and the consolidated fingerprints and scores are figured (Genuine/Imposter).

1.4 Aim and Objectives

The main aim of this research is to create a fingerprint protection by combining two fingerprints into a new identity. In this research, we propose a process for producing a combination of fingerprints using MATLAB.

The main objectives of this research are

- To combine two fingerprints by minutiae position.
- To get more efficiency compared with previous techniques.
- To calculate the similarity between combined and original fingerprint.

1.5 Research Questions

The following are the research questions:

1. How does the combination of two fingerprints effect the minutiae position in the template?
2. How is the proposed algorithm better in terms of similarity score, FMR, FNMR, EER when compared to the existing methods?
3. What is the similarity between the original fingerprint and combined fingerprint?

1.5 Outline of Thesis

Chapter 1: Here we discuss the main aim of this thesis, motivation, aims and objectives, research questions, outline of thesis.

Chapter 2: In this chapter, the background knowledge for good understanding of the thesis is defined in detail step by step.

Chapter 3: In this chapter, fingerprints are explained in detailed.

Chapter 4: In this chapter, the proposed methodology is explained in detailed.

Chapter 5: In this chapter, the performance evaluation factors are explained in detail.

Chapter 6: In this chapter, the results obtained and answers to the research questions are discussed in detail.

Chapter 7: In this chapter, conclusion and future scope are discussed.

In this chapter, the detailed background about fingerprints is discussed.

Fingerprint Enhancement

We have many approaches for enhancing the quality of the image and some recent methods which are following are as follows

Yonghe Tang, Liehui Jiang, Yifan Hou and Ruimin Wang proposed an algorithm that is useful to enhance the contrast between the ridges and valleys of the contactless fingerprints. Their algorithm based on hessian matrix and short Fourier transform (STFT) analysis. This algorithm enhances initially by building hessian matrix filter according to the linear features of a fingerprint ridge and then enhances it on the basis of the texture feature fingerprint. Finally, the final enhancement result is obtained by removing the background noise through fingerprint segmentation. The experimental results show that the proposed algorithm not only can enhance the contrast of fingerprint ridge and valley effectively but also restrain noise and the processing speed is faster[3].

Soweon Yoon, Jianjiang Feng and Anil k. Jain proposed an algorithm for the latent fingerprints to enhance its quality. This enhancement algorithm is to improve the clarity of the ridge structures and therefore make the subsequent processing, such as minutiae extraction and matching algorithm, insensitive to the quality of fingerprint images. This algorithm which is especially for the latent fingerprints to enhance its quality. Local ridge pattern in fingerprints can be approximated well by a 2D sinusoid wave. Based on this fact, 2D Gabor filters have been successfully used for fingerprint enhancement. It consists of two important parameters: local ridge orientation and frequency. with proper choice of these parameters, Gabor filter can connect broken ridges and separated joined ridges. Compared to frequency, ridge orientation is even more important, as the range of possible ridge frequency values is small for adult fingerprints and ridge frequency is often estimated after ridge orientation is known. For this reason, they have focused on the estimation of orientation field in latent images and the core of the proposed enhancement algorithm is an orientation field estimation algorithm, which fits an orientation field model to the course orientation field estimated from skeleton provided by a commercial fingerprint SDK[4].

Miao-li WEN, Yan LIANG, Quan Pan and Hong-Cai ZHANG proposed a Gabor based fingerprint enhancement algorithm in the wavelet domain. Their main aim is to improve the clarity and continuity of ridge and valley structures. It involves 4 steps they are normalization, wavelet decomposition, block orientation estimation and finally using Gabor filter to enhance the fingerprint image in wavelet domain[5].

Feature extraction and fingerprint combination

Prashant Bhaskarrao Patil and Nitin N. Patil proposed an algorithm which has to preprocess a fingerprint image, feature extraction, reference point detection and combination of two fingerprints. After applying pre-processing methods system gets a thinned image, from that a different shape of connection points is appeared called as Crossing Number (CN). There are different types of properties like isolated point, ridge ending point, bifurcation point. Minutia Point has a number of attributes like its location, orientation, type (ridge termination, ridge bifurcation, etc.). The minutiae Point type is called as Crossing Number (CN) and for the combined image generation system has to find a central singular point on both the images which is known as reference point. It is a core point in an image used for alignment. They have proposed 7 stages to generate the combined fingerprint image by estimating the associate degree orientation from the set of trivialities points, generate a binary ridge pattern by using Gabor filters, regenerating the continuous phase image by reducing the spirals in the image, mix the continual part image and also spiral part image manufacturing a reconstructed part image, produce a refined phase image from regenerated phase image by removing spurious minutiae points, apply a unwanted noise and rendering step refined image thus on produce an original-look like thumbprint image[6].

Sheng Li and Alex C. Kot have proposed a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity. In the process firstly, the system captures two fingerprints from two different fingerprints. In the combined template, the minutiae points and directions are extracted from two different fingerprints directly. These minutiae positions and directions share a similar topology to those from an original fingerprint. Therefore, the combined minutiae template has a similar topology to an original minutiae template. To make the combined minutiae template look real as an original minutiae template, three different coding strategies are introduced during the combined minutiae template generation process. Therefore, are able to combine two different fingerprints into a new virtual identity by reconstructing a real-look alike combined fingerprint from the combined minutiae template[2].

For feature extraction, Rabih Nachar and Elie Inaty have proposed a detector to extract the minutiae and the corners as feature points on the edge of a ridge. To do, so They have introduced a new feature segment called straight edge [SE]. Thus, a ridge's edge will be composed of one or more sequential SEs. The head of the first SE and the tail of last SE are minutiae termination or bifurcation.

The interaction between two successful SEs is considered as a corner. In fig. you will observe that C is the corner and it is composed of two SEs, T, H are the two minutiae. In this paper, they have main objective which was to extract a new set of feature points that will lead to a good performance in matching. Minutiae are one of these feature points detected on the edges of the ridges of a fingerprint image. In addition, new feature points are introduced as new characteristics of a Fingerprint. They are the edge corners ECs that characterize the curvature of a ridge edge. The performance of the algorithm was evaluated twice using minutiae with or without

corners and then compared to the performance of other algorithms. As a result, both evaluations were very similar to the evaluations of existing algorithms. However, the performance was better using both feature points: minutiae and corners[7].

Chapter 3

Background

3.1 Fingerprint History

At first, a devised method of body measurements used to classify the individuals and later on Fingerprints have been used to identifying people due to the west case incident happened in a federal prison in Leavenworth. Fingerprinting First created by a British surgeon named Dr. Henry Fault and later on in the late nineteenth century Sir Francis Galton discovered some of the characteristics from which fingerprints can be identified and in 1980's first computer database of fingerprints was developed, which came to be known as the Automated Fingerprint Identification System [AFIS] by FBI and it first connected to National Bureau of Standards (NBS) known as National Institute of Standards and Technology (NIST). At present, we have nearly 700 million individual fingerprints entered in AFIS[8].

3.2 Fingerprint Pattern

Human Fingerprints consists of ridges and valleys as well as the minutiae points, which are the points where the ridge structure changes and these all together form a distinctive and unique pattern. No two people have the same fingerprint pattern and it will remain unchanged for the life of an individual, however, the characteristics of the pattern may change due to the temporary scars and diseases.

But whenever the injuries are fully healed, the same fingerprint will reappear. Figure 3.1 shows the fingerprint characteristics[9].

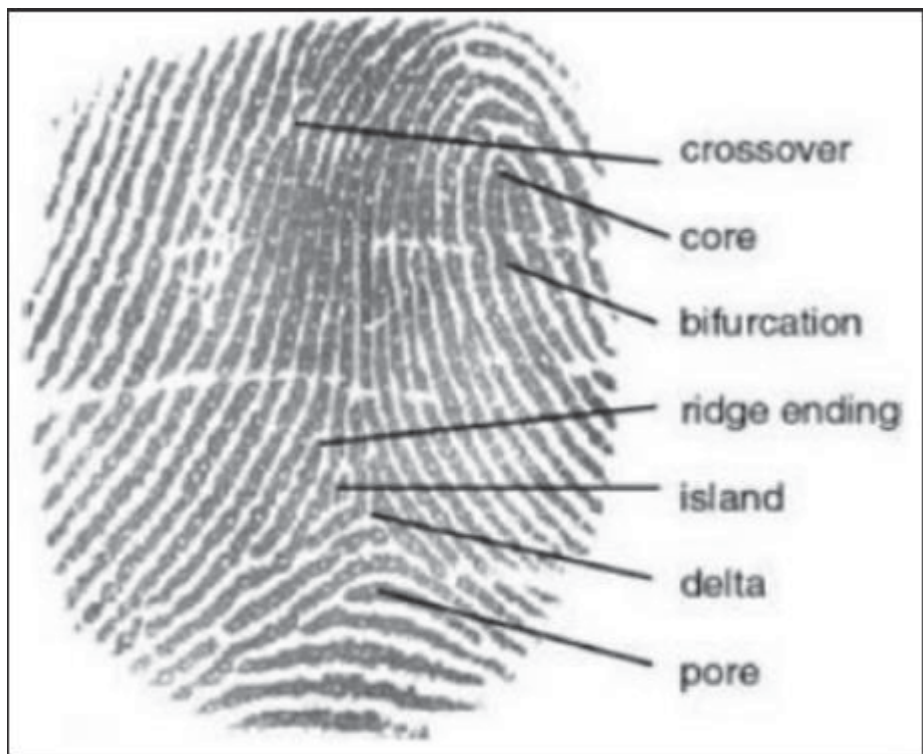


Fig.3.1: Fingerprint characteristics.

Based upon visual pattern fingerprint patterns are divided into three classes, they are Arches, Loops and Whorls[10]. Where arches are the simplest and primary class of fingerprint pattern that is formed by ridges that enter on one side and exit on the other and no deltas are present in this fingerprint and for the loops it has at least one delta and one or more ridge that enter and exit on the same side. Whereas in whorls it has at least two deltas and one ridge that tends to make a complete circle which can be observed in figure 3.2.

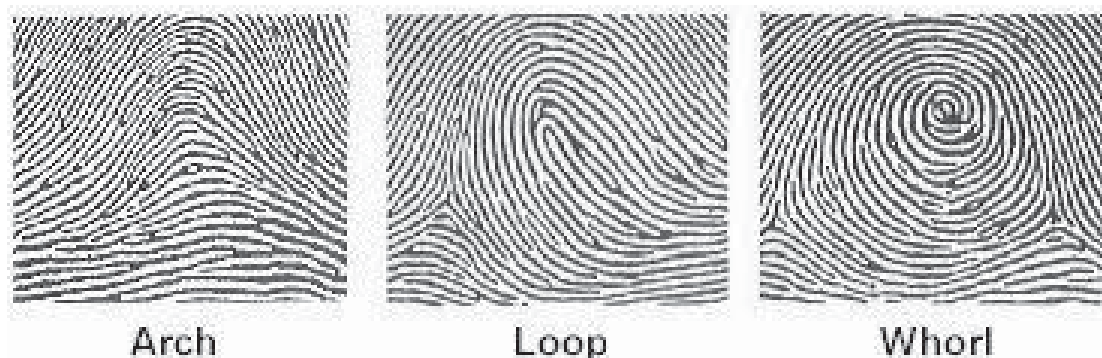


Fig.3.2: Fingerprint Patterns.

With all these, we found that fingerprints are unique and distinctive. When matching or comparing the fingerprint patterns the ridge characteristics are used as a point of identification. The more points you can find in common can get the better match. Figure 3.3 shows the ridge characteristics of the fingerprint[11].

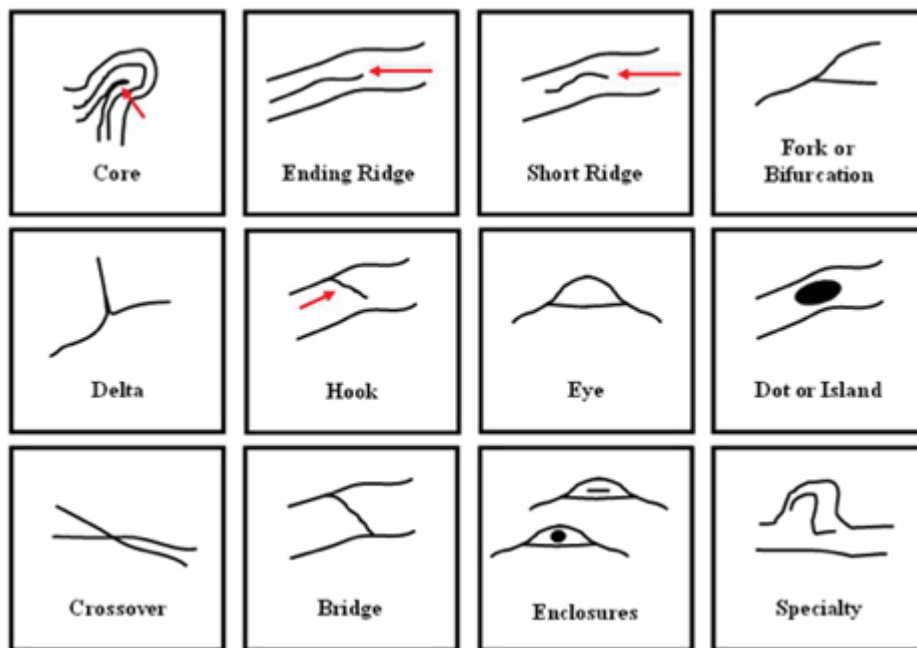


Fig.3.3: Fingerprint Ridge Characteristics.

3.3 Fingerprint Sensing

There are various approaches to obtain the fingerprints are

1. **Latent prints:** there are the left impressions by friction ridge skin on a surface such as a door, glass, tool handle etc.
2. An electronic fingerprint scanner which is used to get the digital copy of the fingerprint pattern. We will have different electronic fingerprint scanners to get an image of somebody's finger like optical fingerprint sensors, capacitive sensors etc. and both types would come up with the same sort of image but getting with different ways[12].
 - a. Optical Fingerprint sensor: the heart of an optical scanner is a charged coupled device (CCD) and it is a light sensor system which is quite used in the camera and camcorders. The scanning process starts when you place your finger on the glass plate, and a CCD camera takes a picture and actually CCD system generates an inverted image of the finger, there the darker positions representing the ridges of the finger and lighter areas representing the valleys between the ridges[12].

- b. Like optical scanners, capacitive fingerprint scanners generate an image of the ridges and valleys to make up a fingerprint but sensing will take place using the electrical current instead of using light.



Fig 3.4: (a) is a latent one and another one (b) which is from the electronic sensing system.

3.4 Fingerprint Database

One of the most important and time-consuming tasks of any biometric system evaluation is the data collection. During performance evaluation, fingerprints belonging to the same database will be matched against each other. In our thesis, we used fingerprint database FVC 2002.

With the aim of track the recent advances in fingerprint verification, for both academia and industry, and to provide up the data to the fingerprint technology after the FVC2000 got the appreciation and encouragements received, induced the organizers to schedule a new competition for 2002 that is Second International Competition for fingerprint verification algorithms [FVC2002][13].

- The databases used in this contest have not been necessarily acquired in a real environment and according to a formal protocol.
- Only parts of the system software will be evaluated by using images from sensors not native to each system.

In FVC2002 we have 4 databases (DB1, DB2, DB3 and DB4) and they were collected by different sensors/technologies. Below table gives the information regarding all databases clearly[13].

TABLE I Sensors and respective Image data

	Sensor Type	Image Size	Set A (wxd)	Set B (wxd)	Resolution
DB1	Optical Sensor	388x374 (142 Kpixels)	100x8	10x8	500 dpi
DB2	Optical Sensor	296x560 (162 Kpixels)	100x8	10x8	569 dpi
DB3	Capacitive Sensor	300x300 (88 Kpixels)	100x8	10x8	500 dpi
DB4	SFinGe v2.51	288x384 (108 Kpixels)	100x8	10x8	about 500 dpi

Each database is 100 fingers wide(w) and 8 impressions per finger deep(d) that is a totally of 800 fingerprints. DB1, DB2 are taken by using optical sensor and DB4 was taken by synthetic fingerprint generation.

The sample images from each database are as shown in figure 3.5[13].



Fig 3.5: Sample Images from each Data Base

Performance evaluation

To know the genuine fingerprints, they have done the false non-match rate [FMNR] it is also referred as false rejection rate- FRR. There each sample is a subset A is matched against the remaining samples of the same fingerprint. From that, the total number of genuine tests is 2,800.

To compute the false acceptance rate, the first sample of each finger in the subset A is matched against the first sample of the remaining fingers in A. There should be a total number of false acceptance tests is 4,950.

3.5 Fingerprint Recognition

In the fingerprint recognition system, we would see the different modules for verifying the fingerprint and in the automated fingerprint recognition system there are fingerprint classification and the matching are the key parts. For the matching, there would be various approaches like minutiae based, image based are used to

compares the features from the input fingerprint features against all the appropriate records in the database to determine if a probable match exists or not. Among those approaches, minutiae based was the popular one in the contemporary fingerprint identification and verification system[14].

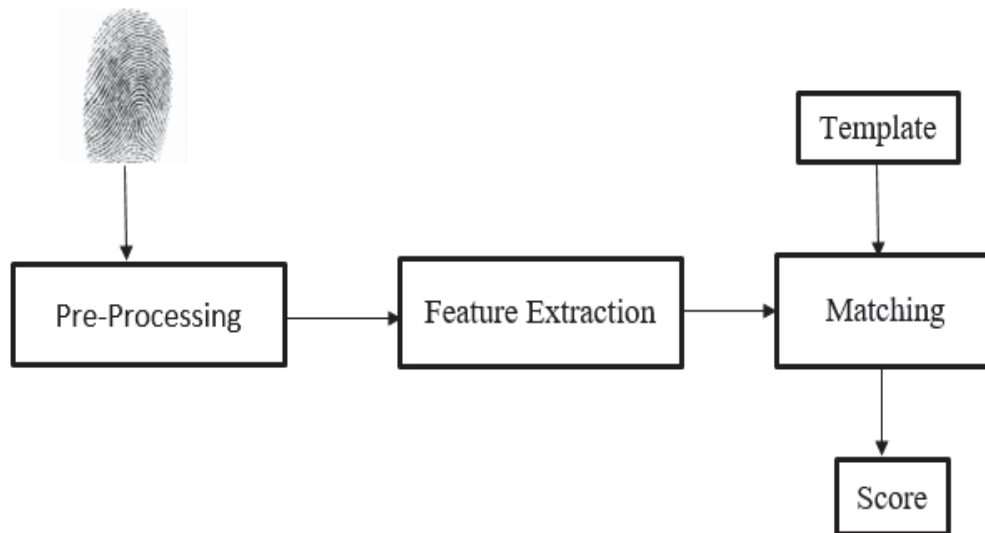


Fig.3.6: Main modules of a fingerprint verification system.

Figure 3.6 shows the main modules involved in an Automatic fingerprint recognition system[14].

Pre-processing: here the fingerprint has been enhanced and adapted to simplify the task of feature extraction.

Feature extraction: here the fingerprint is further processed to generate discriminative properties, also called feature vectors.

Matching: here the feature vector of the input fingerprint is compared to one or more existing templates. The templates of approved users of the biometric system, also called clients, are usually stored in a database.

A similarity score is generated between the fingerprints and if the similarity score is above acceptable limit fingerprint is identified.

Chapter 4

Proposed Method

This chapter deals with the proposed fingerprint combination and other stages involved before and after combination.

4.1 Overview of Proposed Method

The fingerprint image from the FVC database is first preprocessed to enhance the contrast and to remove the noise present in the image then the image is rotated using eigen vectors and then minutiae are extracted from fingerprint image a postprocessing operation is performed on the minutia extracted finally fingerprints are combined.

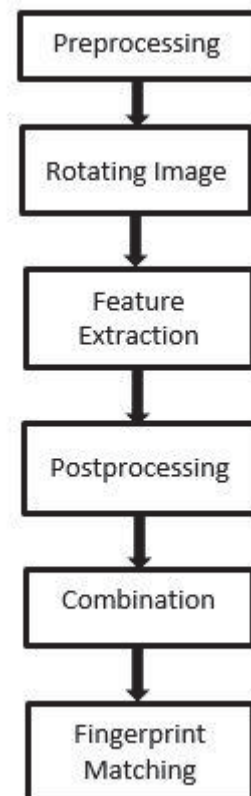


Figure 4.1: Overview of Proposed Model

Figure 4.1 shows the overview of the proposed method. The following sections will give a brief outlook about all the blocks in the flowchart.

4.2 Pre-Processing

Pre-processing of the fingerprint images is done to remove the noise present in the fingerprints and to increase the quality of fingerprint characteristics like ridges and bifurcations, it improves the matching scores and helps in finding minutiae positions of a fingerprint accurately.

Fingerprints are acquired using various scanners; quality of fingerprints depends on scanners and finger. Noise in the fingerprint can be introduced by various factors like pressure applied on the scanner while acquiring fingerprints, injuries and wrinkles on the fingerprints, low contrast due to dryness of the finger and so on[15]. Matching and verification of fingerprint in an automated fingerprint identification system depends upon proper detection and extraction of its features, firstly the noise in the fingerprint is removed and the image is enhanced to improve the clarity of the ridges and valley structures, enhancement of low quality fingerprints helps in detection of minutiae positions without spurious features. However, the results of preprocessing greatly affect the quality and the ability to make a match.

Preprocessing can be done by various methods, in this thesis we implemented adaptive histogram equalization to increase the contrast of the image and the noise in the fingerprint image is removed by preventing of amplification of noise by limiting over amplification of intensities.

4.2.1 Histogram Equalization

The histogram of a digital image is a distribution of pixels according to their intensities in the range of $[0, L-1]$ where L is number of gray values in the image[16].

Histogram of a grayscale image with L possible gray levels, $i = 0, 1, \dots, L-1$ is calculated as

$$P(i) = \frac{n_i}{N}. \quad (4.1)$$

Where n_i is the number of pixels with gray level i , N is the total number of pixels in the image[17].

Histogram normalization is a technique in which each value of the histogram is divided by the number of pixel in the image to convert discrete distribution of intensities in a histogram into a discrete distribution of probabilities. Histogram axis is normalized between 0 and 1.

Histogram equalization is used to increase the contrast of the image by modifying the intensity distribution of the histogram by evaluating the probability of every level and then reassigns a new level based on this probability which results in a flat histogram.

Histogram equalization relies on Cumulative Distribution Function (CDF),

which is a cumulative sum of probabilities lying in its domain,

$$cdf(i) = \sum_{j=0}^i P(j). \quad (4.2)$$

This gives a linear CDF in the resulting image, however linear CDF is associated to the uniform histogram[16].

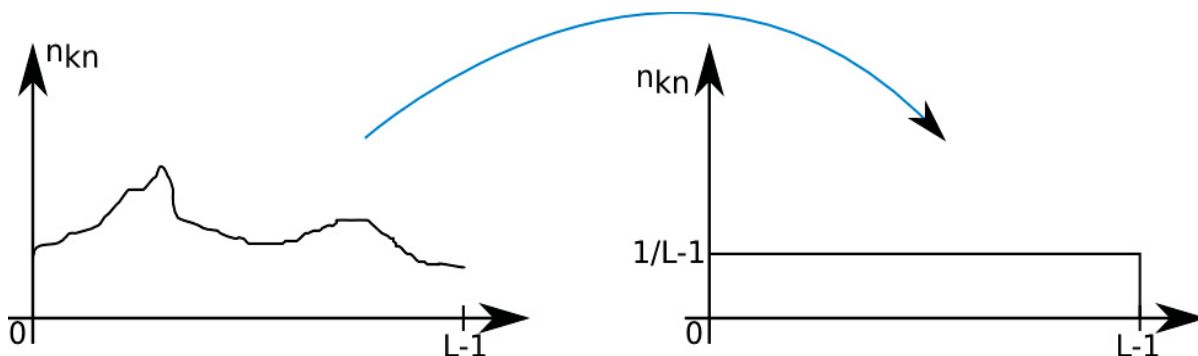


Figure 4.2: Technique to perform histogram equalization

The value of cumulative distribution function at the k^{th} intensity level (S_k) of the resulting image can be given as

$$S_k = (L - 1) \sum_{j=0}^k \left(\frac{n_j}{N} \right). \quad (4.3)$$

Where $k=0,1,2,\dots,L-1$.

Histogram equalization increases the contrast of the fingerprint images, but the disadvantage of using the histogram is that it also increases the contrast of the noise along with the fingerprint image. To overcome this drawback an adaptive histogram equalization is adopted in this thesis called Contrast Limited Adaptive Histogram Equalization (CLAHE) it prevents over amplification of noise by limiting the amplification of intensities which ensures uniform contrast throughout the image[18]. From the figure 4.3 we can see that the contrast of the input fingerprint image is increased.



Figure 4.3: Enhanced Image

4.2.2 Binarization

The grayscale fingerprint image is converted to binary image, as binary image increases the accuracy of minutiae detection in fingerprints, binarization is a method where grayscale image (0 to 256 levels of gray) is converted into black and white image (0 or 1) using a threshold, every pixel in the fingerprint image is compared with the threshold, whose values are more than the threshold are converted to white pixels and whose value are less or equal to the threshold are converted to black pixels[19], the resulting binary image can be given as

$$BW(n_1, n_2) = \begin{cases} 1, & \text{if } I(n_1, n_2) > T_p \\ 0, & \text{otherwise} \end{cases} \quad (4.4)$$

Where, $BW(n_1, n_2)$ is the resulting binary image, T_p is the threshold, $I(n_1, n_2)$ is the intensity of pixel at position (n_1, n_2) .

4.2.3 Thinning

Minutiae positions from a fingerprint can be easily obtained by skeletonizing the image as it reduces the complexity to develop minutiae extraction algorithm by reducing the pixel width of the ridges to a single pixel width and helps in the faster computation of minutiae positions[20].

Thinning of a fingerprint can be obtained by performing morphological operations on the binary image obtained above. A morphological operation called dilation is applied to the image until no further changes can occur which results in a ridge thickness of 1-pixel width figure 4.4 shows the thinned image obtained after processing.



Figure 4.4: Thinned Image

4.3 Rotation of Fingerprint Image

From the figure 4.5 we can see that the fingerprints obtained in real time are often not straight this happens due to many factors like the width of the scanner, dryness of finger, human error and so on. The combination of two fingerprints in this thesis is based on 50:50 the combined template consists of left side of the first fingerprint from the center and the right side of the second fingerprint from the center to make this possible we should have the fingerprints based at the same location and direction, the images obtained in real time may be tilted to overcome this we need to rotate the image.



Figure 4.5: Fingerprints obtained in real time

Rotation of fingerprint is done by finding the angle of the rotation of the image using eigen vectors for which we need to find the center of the fingerprint for this purpose the fingerprint is masked to separate the fingerprint from the image background which introduced by the scanner.

4.3.1 Fingerprint Masking

Fingerprint form only small part of the fingerprint image, with masking we can retain only the fingerprint and remove all the unwanted part in the fingerprint image[21].

Bwconvhull:

The issue of finding convex hull discovers its reasonable applications in design acknowledgment, picture preparing, measurements, geographic data framework, diversion hypothesis, development of stage graphs, and static code investigation by theoretical elucidation. It likewise fills in as an instrument, a building obstruct for various other computational-geometric calculations, for example, the pivoting calipers strategy for registering the width and distance across of a point set.

In arithmetic, the arched structure or raised envelope or curved conclusion of a set X of focuses in the Euclidean plane or in a Euclidean space is the littlest raised set that contains X . For example, when X is a limited subset of the plane, the raised frame might be imagined as the shape encased by an elastic band extended around X .

Formally, the arched body might be characterized as the crossing point of every single curved set containing X or as the arrangement of every single raised mix of focuses in X . With the last definition, arched bodies might be stretched out from Euclidean spaces to self-assertive genuine vector spaces; they may likewise be summed up further, to situated matroids.

Masking is an image processing technique masked image is simply a binary image in which the region of interest (ROI) represents value 1 and the background represent value 0[22].

To mask a fingerprint image the ROI should be identified for this purpose we used histogram discussed in section (4.2.1), to find the no of levels of gray in the fingerprint image as shown in the figure 4.6 and created a binary mask by converting all the values in the region as pixel value 1 and the remaining pixels to value 0, from this binary image a convex hull image (i.e. convex hull is the smallest polygon of pixels that surround all the white pixels in the input[23]) is generated using `bwconvhull(BW)` function in matlab where `BW` is binary image[24].

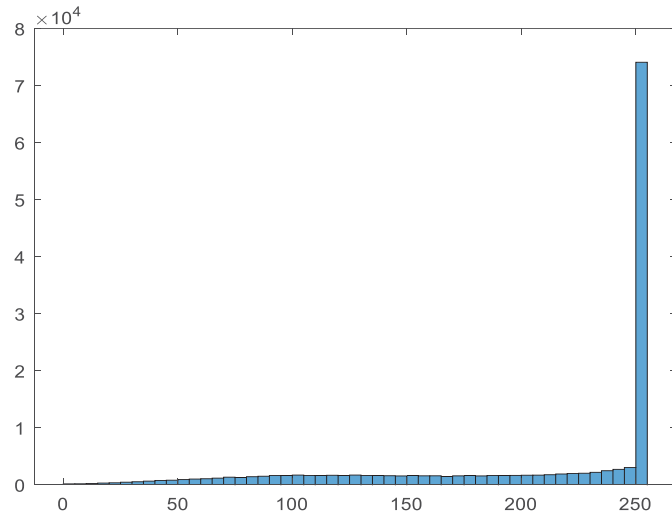


Figure 4.6: Histogram of Fingerprint Image

From the figure 4.7, we can observe that a mask is generated for the fingerprint image. Now to rotate the fingerprint image we need to find the eigen vectors and the rotate the image counter clockwise to make the fingerprint image straight.

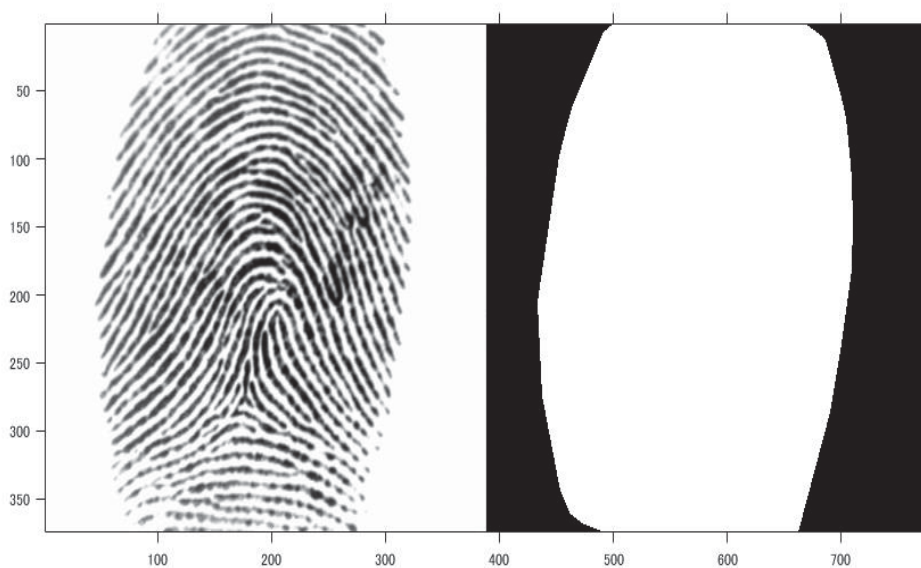


Figure 4.7: Binary Mask of fingerprint image

4.3.2 Eigen Values and Eigen Vectors

The eigen value problem is to determine the solution to the equation $A\mathbf{v} = \lambda\mathbf{v}$, where A is an n -by- n matrix, \mathbf{v} is a column vector of length n , and λ is a scalar[25].

The values of λ that satisfy the equation are the eigen values. So,

$$\begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{bmatrix}. \quad (4.5)$$

If it occurs that matrix \mathbf{v} and ω are scalar multiples, that is if

$$\mathbf{A}\mathbf{v} = \omega = \lambda\mathbf{v}. \quad (4.6)$$

Where, \mathbf{v} is an eigenvector of the linear transformation \mathbf{A} and the scale factor λ is the eigenvalue corresponding to that eigenvector. Equation (4.6) is the eigenvalue equation for the matrix \mathbf{A}

$$\mathbf{A}\cdot\mathbf{v}=\lambda\cdot\mathbf{v}, \quad (4.7)$$

$$\mathbf{A}\cdot\mathbf{v}-\lambda\cdot\mathbf{v}=0, \quad (4.8)$$

$$\mathbf{A}\cdot\mathbf{v}-\lambda\cdot\mathbf{I}\cdot\mathbf{v}=0, \quad (4.9)$$

$$(\mathbf{A}-\lambda\cdot\mathbf{I})\cdot\mathbf{v}=0. \quad (4.10)$$

If \mathbf{v} is non-zero, this equation will only have a solution if $|\mathbf{A}-\lambda\cdot\mathbf{I}|=0$.

Where, \mathbf{I} is the n by n identity matrix.

This equation is called the characteristic equation of \mathbf{A} and is an n^{th} order polynomial in λ with n roots. These roots are called the eigenvalues of \mathbf{A} . We will only deal with the case of n distinct roots, though they may be repeated. For each eigenvalue, there will be an eigenvector for which the eigenvalue equation is true

$$|\mathbf{A} - \lambda\mathbf{I}| = (\lambda_1 - \lambda)^{\mu_A(\lambda_1)}(\lambda_2 - \lambda)^{\mu_A(\lambda_2)} \dots (\lambda_d - \lambda)^{\mu_A(\lambda_d)}. \quad (4.11)$$

We get all the eigen values from the equation.

The algebraic multiplicity $\mu_A(\lambda_i)$ of the eigenvalue is its multiplicity as a root of the characteristic polynomial, that is, the largest integer k such that $(\lambda - \lambda_i)^k$ divides evenly that polynomial.

Eigenvalue option, specified as 'vector' or 'matrix'. This option allows you to specify whether the eigenvalues are returned in a column vector or a diagonal matrix. The default behaviour varies according to the number of outputs specified:

- If you specify one output, such as $\mathbf{e} = \text{eig}(\mathbf{A})$, then the eigenvalues are returned as a column vector by default.
- If you specify two or three outputs, such as $[\mathbf{V}, \mathbf{D}] = \text{eig}(\mathbf{A})$, returns diagonal matrix \mathbf{D} of eigen values and matrix \mathbf{V} whose columns are corresponding eigen vectors[25].

$\lambda_1, \lambda_2, \lambda_3, \dots$ etc are the eigen values and are in diagonal matrix \mathbf{D}

$$\mathbf{D} = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{bmatrix}. \quad (4.12)$$

Here we calculate eigen vectors and eigen values for the autocorrelation matrix to find out the phase angle to which the fingerprint should be rotated.

atan2d

Four-quadrant inverse tangent in degrees. The four-quadrant inverse tangent figure 4.8, $\text{atan2d}(Y,X)$, returns values in the closed interval $[-180,180]$ based on the values of Y and X as shown in the graphic[26].

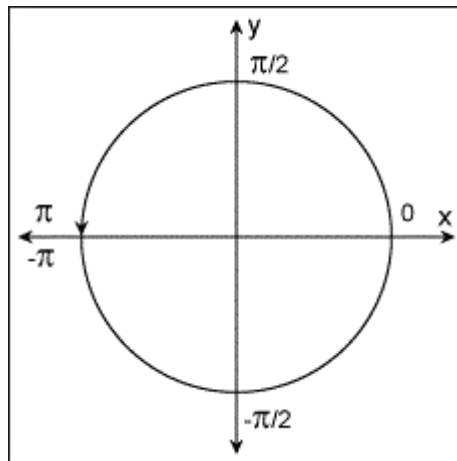


Fig.4.8. Quadrants with phase angles

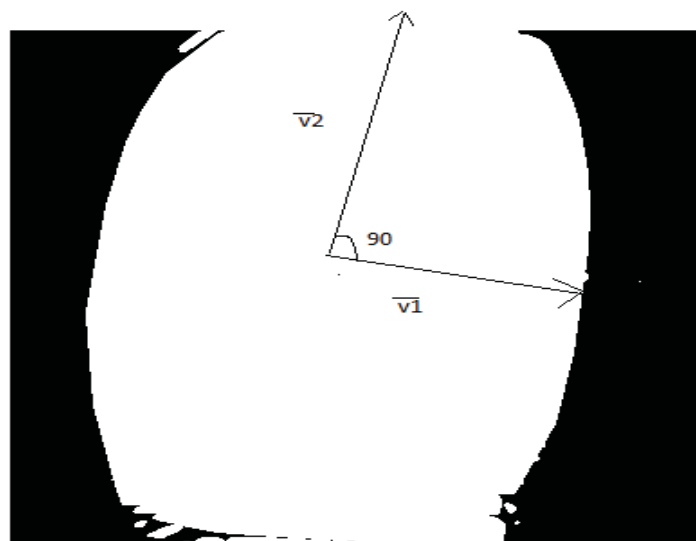


Figure 4.9: Fingerprint mask with imaginary eigen vectors

Figure 4.9 shows the mask of the fingerprint image before rotation, using eigen vectors we can transform the image straight as shown in figure 4.10 by rotating the image at an angle which is found as mentioned.

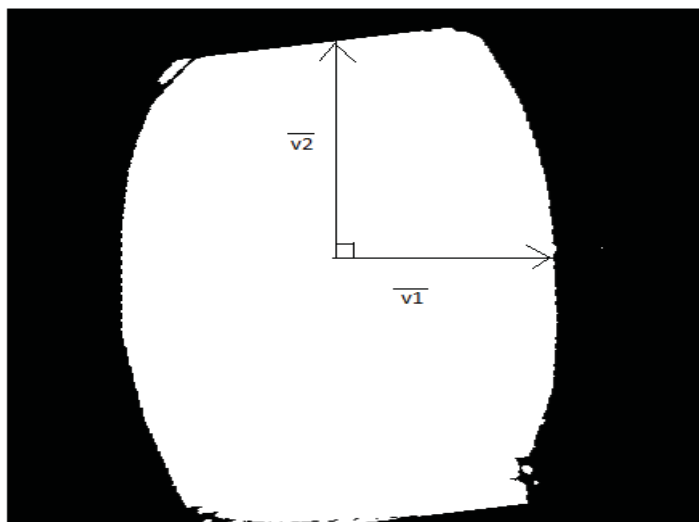


Figure 4.10: Rotated fingerprint mask

Figure 4.10 shows the fingerprint mask after rotation using eigen vectors. From this mask, the center of the fingerprint is found by calculating the row and column mean of the coordinates present in the mask.

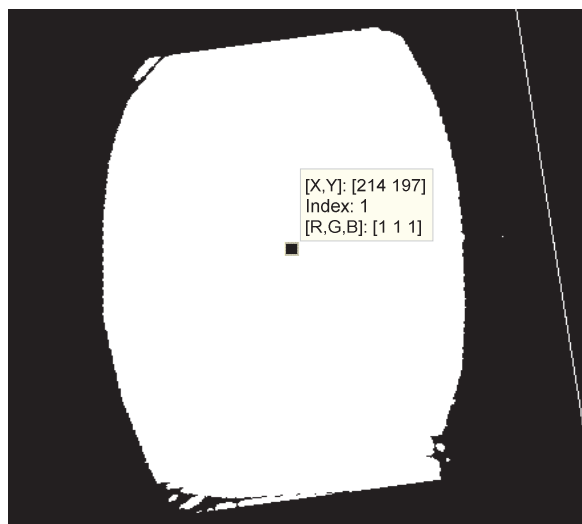


Figure 4.11: Rotated Fingerprint center

Figure 4.11 shows the masked image after rotation with the center of the fingerprint, which is later used to shift the center of the fingerprint to the origin as described in section (4.6).

4.4 Feature Extraction

Fingerprints are unique from one another, minutiae are the point of interest in the fingerprints such as bifurcations and ridge endings the number of minutiae positions differ from one finger to another. Generally, there are somewhere in the range of 30 to 100. When the features are extracted from fingerprints the exact location of minutiae is stored in the form of numerical coordinates along with the phase and quality which can be stored in the database.

Minutiae is described by four parameters,

$$M = (x, y, \theta, q). \quad (4.13)$$

Where x, y = coordinates of the minutiae points, θ = orientation of minutiae points, q = quality of the minutiae points.

Extracting Minutiae from Fingerprint image is one of the most important steps in AFIS. Fingerprint matching algorithms use the details in the minutiae of a finger and compare it with minutiae of another finger and return a matching score.

After the preprocessing block, the enhanced fingerprint images are used to extract minutiae from the fingerprints, in this thesis minutiae are detected and extracted using NIST Biometric Image Software (NBIS) developed by National Institute of Standards and Technology (NIST)[27].

4.4.1 Minutiae Detection and Extraction

NBIS software scans the fingerprint and detects the minutia points and stores the precise location of the minutiae along with the orientation of the minutiae and their quality.

NBIS Software

The Non-export controlled NBIS software includes five packages namely (PCASYS, MINDTCT, NFIQ, AN2K7, and IMGTOOLS), MINDTCT package consists of minutiae detection system which is used in this thesis to detect and extract minutiae from fingerprints[28].

This system takes fingerprint image and detects the minutiae by pointing to the locations at which ridges end or split and their location, orientation, quality.

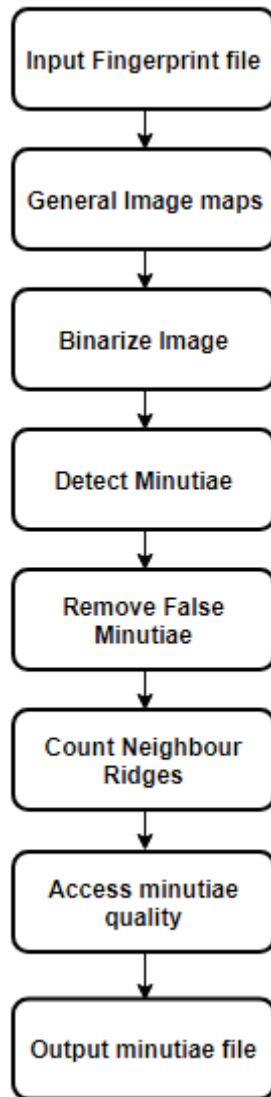


Figure 4.12: Flowchart of steps followed in minutiae detection

The Figure 4.12 shows the steps followed by MINDCT to extract minutiae from the fingerprints.

The minutiae detection algorithm is developed to work on the binary image, so the input fingerprint image should be binarized where black pixels represent ridges and white pixels represent valleys. Then the binary image is scanned to identify localized pixel patterns that show ridge ends or splits which are detected by scanning consecutive pair of pixels for sequences that match the pattern, the scanning is done both vertically and horizontally. A 2×3 pattern is used which contains six binary pixels. The figure 4.13 represents the series of patterns used in this algorithm to detect the minutiae[29].

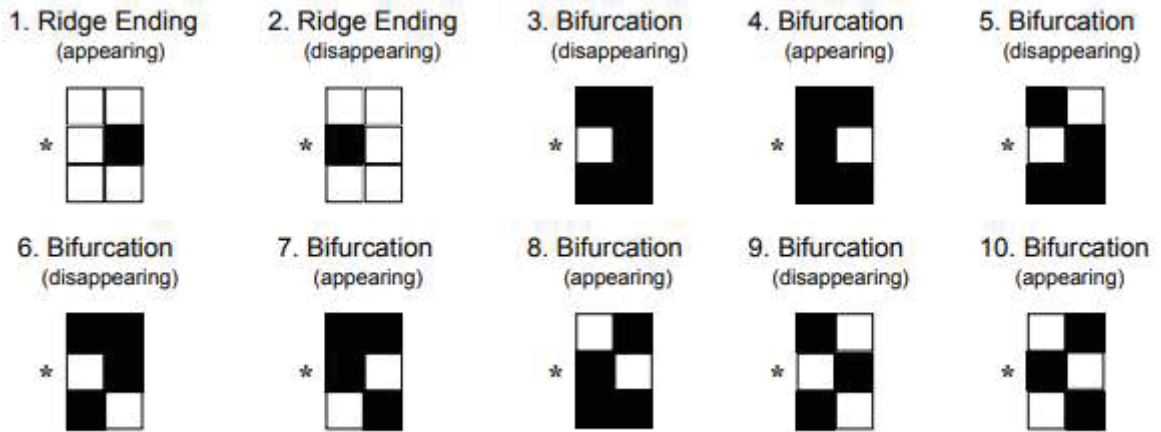


Figure 4.13: Pixel patterns for the detection of minutiae.

In the figure 4.13 the first two patterns represent ridge ending and rest represent bifurcations, another attribute called appearing/disappearing is assigned to each pattern which gives the direction from which the ridge or valley protruding into the pattern[29]. All the pixel pair patterns which match these patterns are identified as minutia points. Figure 4.14 shows the detected minutiae positions in which Green Dots represent Ridge Bifurcations and Red dots represent Ridge Endings.



Figure 4.14: Detected Minutiae points

4.4.2 Location and Orientation of Minutia points

After detecting the minutia points the location and orientation should be calculated which is stored in the database as numerical values. The locations of each minutia point in ANIS/NIST standard specifies the unit of distance as 0.01 mm from an origin in the bottom left corner of the image[30].

For example, consider a 500×600-pixel fingerprint image scanned at 19.69 pixels per mm has dimensions of 25.39×30.47 mm which is standard units of 0.01 mm is

$$2539 \times 3047 = \frac{500}{19.69 \times 0.01} \times \frac{600}{19.69 \times 0.01}. \quad (4.14)$$

The pixel coordinate (235, 210) will be represented in standard units as

$$(1193, 2836) = \left(\frac{235}{19.69 \times 0.01}, 3047 - 1 - \frac{210}{19.69 \times 0.01} \right). \quad (4.15)$$

The y coordinate is measured from the bottom of the image upward.

The orientation of the minutiae is also one of the important factors in any AFIS. The orientation is represented in degrees which is found by calculating the angle between the horizontal axis placed at zero degrees to the right of the minutiae and the line starting at minutia point and running through the middle of the ridge in counter clockwise direction, whereas in the case of bifurcation the orientation is found out by measuring the angle between the horizontal axis and line starting at the minutia point and running through the middle of the intervening valley between the bifurcating ridges[30]. The figure 4.15 depicts the calculation of orientation for ridges and bifurcations[30].

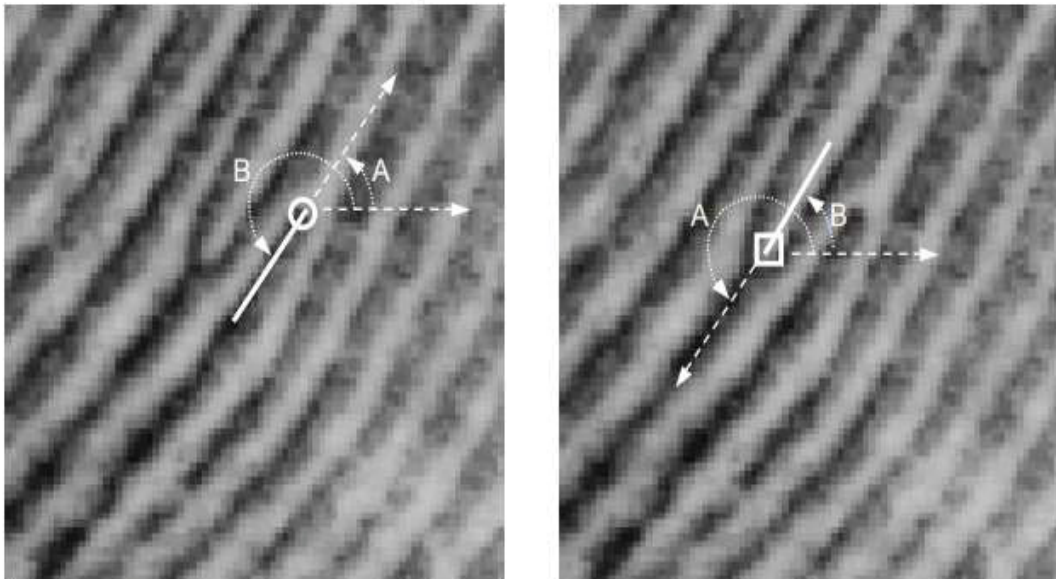


Figure 4.15 Minutiae orientation
A. Standard Angle, B. FBI/IAFIS Angle

4.5 Post-Processing

The minutiae detected contains true and spurious minutiae due to the 6-pixel pattern scan approach used in detection, now the spurious minutiae should be removed without removing the true minutiae as they effect the fingerprint matching rate.

The spurious minutiae are removed using a quality factor, each detected minutia is assigned a value, this is done taking the 'L' the location of minutiae in the quality map of the fingerprint image is assigned a value between 0 and 4 where 0 represents low quality and 4 represent high quality then depending upon the pixel intensity statistics (mean and standard deviation) within in the immediate neighborhood of minutiae is set to 11 pixels, an L= 4 region in fingerprint image will have good

contrast to cover full grayscale spectrum[30].

Reliability (R) from equation (4.16) is calculated using the neighborhood mean μ and standard deviation σ , for an ideal neighborhood the mean is close 127 and standard deviation is ≥ 64

$$F_{\mu} = 1.0 - \frac{|\mu-127|}{127}, \quad (4.16)$$

$$F_{\sigma} = \begin{cases} 1, & \sigma < 64 \\ \frac{\sigma}{64}, & \text{otherwise,} \end{cases} \quad (4.17)$$

$$R = \min (F_{\mu}, F_{\sigma}). \quad (4.18)$$

Where, F_{μ} is the average approximation for mean and F_{σ} is the average approximation for standard deviation in between 0 and 1.

Now the Quality of minutiae(Q) is calculated using Reliability and quality map level L, as following

$$Q = \begin{cases} 0.50 + (0.49 * R) & \text{if } L = 4 \\ 0.25 + (0.24 * R) & \text{if } L = 3 \\ 0.10 + (0.14 * R) & \text{if } L = 2. \\ 0.05 + (0.4 * R) & \text{if } L = 1 \\ 0.01 & \text{if } L = 0 \end{cases} \quad (4.19)$$

The Quality values will be in between 0.01 to 0.99, a high value represent a minutia detected in high quality region and vice versa. Using which true minutiae are retained and spurious minutiae are removed[30].

4.6 Shifting and Combination

The combination of two fingerprints are done using the extracted minutiae positions to the combination is carried out by adding two fingerprints in such way that the left side of the first fingerprint from the center of the fingerprint with the right side of the second fingerprint from the center the combined template has 50:50 characteristics of both fingerprints.

Figure 4.16 shows the minutiae distribution of the first fingerprint and figure 4.17 shows the minutiae distribution of the second fingerprint from the figures we can see it is very difficult to combine fingerprints as minutiae distributions are not equidistant from the origin to combine in 50:50 scheme we need to shift the center of both the fingerprints to origin so that we can combine them easily.

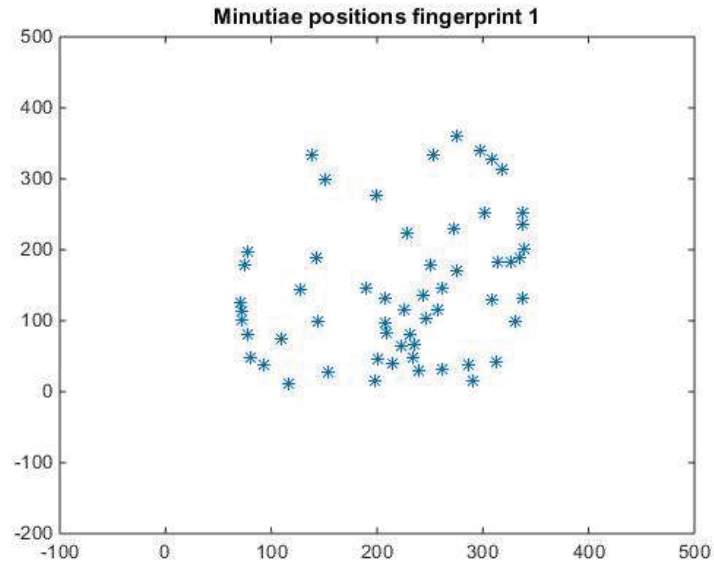


Figure 4.16: Minutiae distribution of fingerprint 1

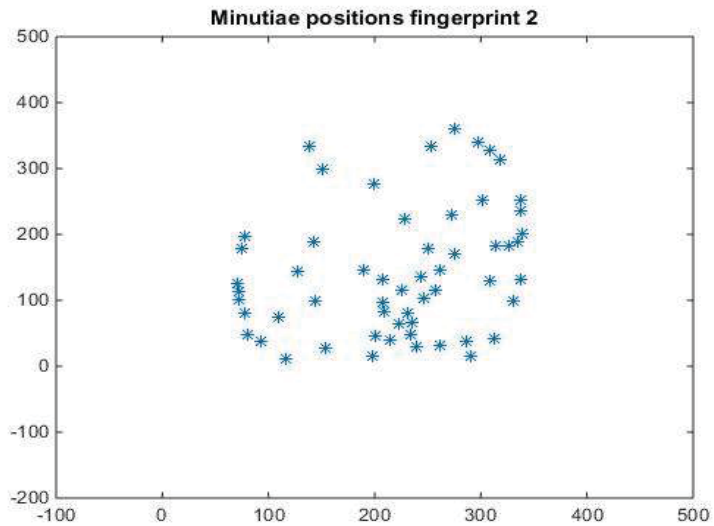


Figure 4.17: Minutiae distribution of fingerprint 2

To shift the center of the minutiae positions to origin we need to subtract the mean of the minutia from all the individual minutiae positions. The mean of the minutiae can be calculated as

$$Mean(x, y) = \frac{\text{sum of all minutia cordiantes}(x,y)\text{in a fingerprint}}{\text{number of minutiae points}}. \quad (4.20)$$

Figure 4.18 shows shifted minutiae distributions and 50% of the fingerprint minutiae distribution considered from both the images, after the center of the fingerprint is shifted combination is carried out according to the above scheme.

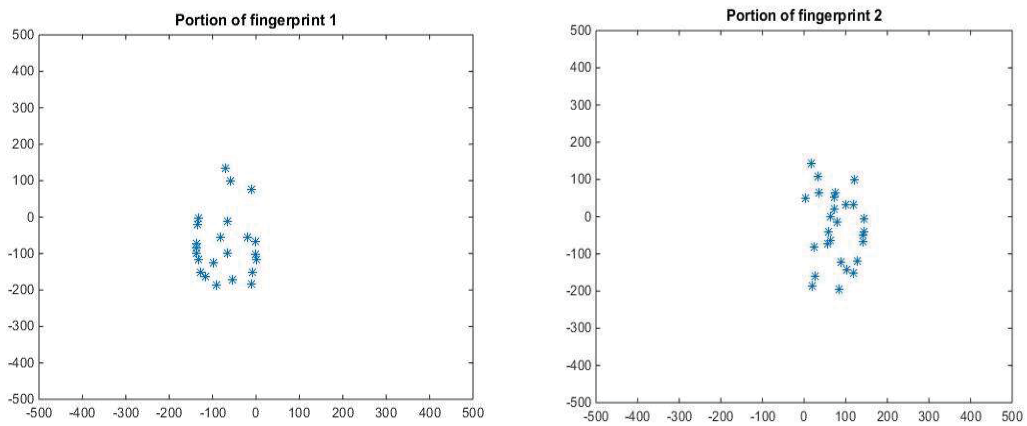


Figure 4.18: Minutiae distribution of both fingers after shifting center and 50% used for combination

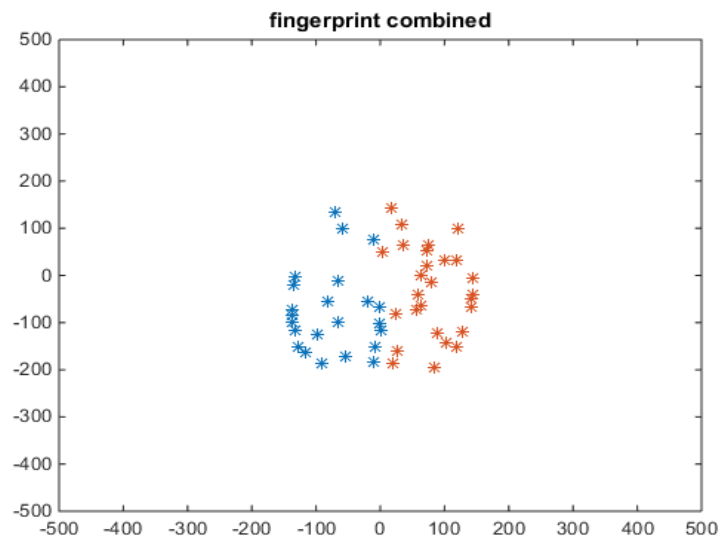


Figure 4.19: Minutiae distribution of combined fingerprint

Figure 4.19 shows the minutiae distribution of the combined fingerprint, this same process is carried out for all the fingerprints in the FVC2002 db1a database which consists of 100 different fingerprints images from which 50 combined fingerprint templates are obtained.

4.7 Fingerprint Matching

AFIS uses fingerprint match score between two fingerprints (one stored in the database with the query fingerprint). The score will be high if the matching is done between same fingerprints which are called genuine match and score will be less if the matching is done between two different fingerprints and is called imposter match.

The match score highly depends upon features extracted from the fingerprint. There are several factors which result in bad match score they are

- Intraclass variations (variations in same fingerprint images) and Interclass similarity (similarity between same fingerprint images).
- Residues from previous fingerprint acquisition.
- Finger pressure, placement and contact area in accordance with the scanner.
- Condition of the finger – cuts, dryness, sweat and humidity on the finger while acquisition.

The fingerprint matching techniques/ algorithms are based upon one of the following four methods image correlation, phase matching, skeleton matching, and minutiae matching. In this thesis, we adopted the minutiae matching technique for fingerprint matching as it reliable, uses less memory and provides faster computation speeds[31].

In a minutia based matching, the matching is done on 30-100 minutiae detected on a typical fingerprint rather than the 250,000 pixels in the fingerprint image [28]. We used a NIST developed feature matching algorithm BOZORTH3 (export controlled), which matches two minutia patterns and returns a match score.

Minutia based matching algorithm are generally developed based on four steps they are [31]

- Similarity between minutiae of two fingerprints of two fingerprints by comparing minutiae descriptors that are invariant to rotation and translation are computed pair wise.
- Fingerprints are aligned according to most similar minutiae pair.
- Corresponding minutiae that are close enough in both location and direction are noted.
- Finally, the algorithm outputs the similarity score based on the number of matching minutiae, consistency of ridge count between matching minutia and percentage of matching minutiae in the overlapping region of two fingerprints.

The genuine and imposter matching scores obtained while matching two combined fingerprints and individual query fingerprint against combined fingerprint template using above algorithm are discussed briefly in chapter 6.

Chapter 5

Performance Evaluation

The term “Biometric” is made up of two words: “Bio” indicates that the subject concerns living things. “Metric” indicates that the subject involves quantitative measurements in a mathematical sense.

5.1 Biometric classification

Utilizing some metric, a biometric verification calculation ordinarily delivers a similarity score each time two examples (particulars of unique mark pictures) are thought about. Finish understanding between two pictures may, for instance, render a score of "one", and finish contradiction may render a score of "zero". Genuine correlations normally render a similarity score in the between. With a specific end goal to characterize the pictures as either originating from one and a similar individual or not (that is, a parallel order) the calculation commonly limits against a set edge esteem T [32].

Traditionally, the measurements utilized as a part of unique finger impression construct confirmation depend with respect to the relative positions found for the details. Exact Biometrics' measurements depend on pixel-by-pixel correlations in bitmaps of trademark districts of the unique finger impression, be that as it may.

Two types of errors are related with paired characterization. An unapproved person may wrongly be distinguished as being approved, and an approved individual may wrongly be distinguished as being unapproved. The previous sort of blunder is known as a "false acceptance", the last a "false rejection". The rate at which these mistakes happen, the False Acceptance Rate (FAR) and the False Rejection Rate (FRR), are imperative measures of the "grouping quality" of a confirmation calculation. The two rates rely upon the edge T decided for an arrangement. In this manner, FAR and FRR are reliant, as e.g. represented by a Receiver Operating Characteristic (ROC) curve[33], which plots FRR against FAR.

5.2 Performance evaluation factors

5.2.1 False Acceptance Rate (FAR)

The FAR is the rate at which a biometric confirmation framework incorrectly validates information as having a place with a specific approved person.

The FAR might be seen as a security parameter. In the event that a calculation is great at finding contrasts between two examples, this is reflected in a low FAR. Two sorts of assault will here delineate the FAR's part as a security parameter: An

interloper may endeavor to assault a biometric security framework for instance through a "zero-effort" assault or a "brute force" attack. A "zero-effort" attack comprises of setting ones possess finger on the sensor to test whether the framework truly can discover enough contrasts concerning an approved individual to deny get to. The FAR may, therefore, be converted into the danger of a fruitful zero-exertion attack.

The false accept rate is the percentage of invalid inputs that are incorrectly accepted can be calculated as

$$FAR = \frac{\text{Total number of imposter fingerprints accepted as genuine}}{\text{Total number of tests pergormed}}. \quad (5.1)$$

5.2.2 False Rejection Rate (FRR)

The FRR is a parameter for a biometric framework. It depicts the rate at which an approved individual is rejected. The approved client encounters denied access as annoying.

The FRR depends intensely on client conduct and sensor innovation. An unpracticed Client may tend to exhibit distinctive segments of the finger to the sensor, and a lower quality sensor has a tendency to lose a greater number of subtle elements of the example than a more expensive variant.

The false reject rate is the percentage of valid inputs that are incorrectly rejected can be calculated as

$$FRR = \frac{\text{Total number of genuine fingerprints rejected as imposters}}{\text{Total number of tests pergormed}}. \quad (5.2)$$

5.2.3 Equal Error Rate (EER)

The EER demonstrates the precision of the framework. The false acceptance rate and false rejection rate cross at one point which is known as the EER[32] (the point in which the FAR and FRR have a similar esteem) as shown in figure 5.1.

In principle, the right clients ought to dependably score higher than the impostors. A single edge could then be utilized to isolate the right client from the impostors. All in all, the coordinating calculation plays out a choice in view of an edge which decides how near a format the info should be for it to be considered a match. In the event that the edge is diminished, there will be less false non-matches in any case, falser acknowledges.

Correspondingly, a higher limit will lessen the false acknowledge rating yet increment the false reject rating. In a few cases, impostor designs produce scores that are higher than the examples from the user. For that reason, that however the edge is picked, some grouping blunders happen.

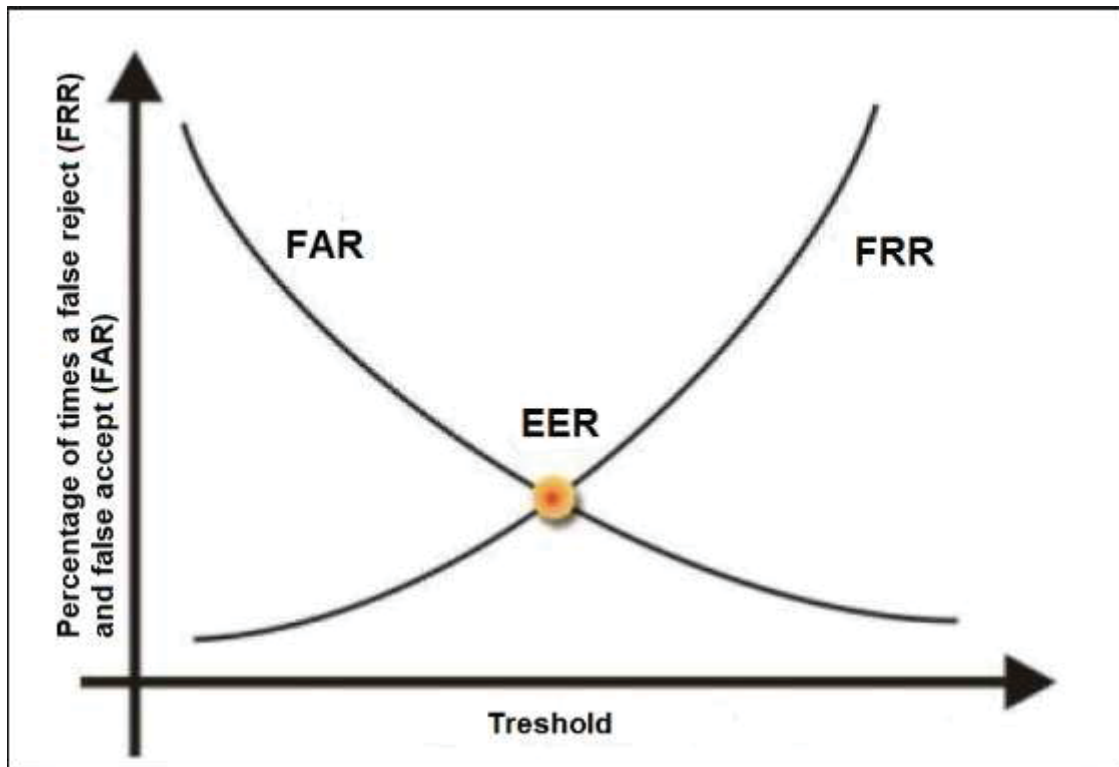


Figure 5.1: Sample Curve indicating EER

Chapter 6

Results and Discussion

This chapter deals with the results and the effects of the results and also deals with the answers to the research questions and problem faced during the implementation.

6.1 Results

We have combined hundred different fingerprints from FVC2002 Db_1a into fifty combined fingerprint templates from which we have calculated the Genuine and Imposter scores.

6.1.1 Genuine Scores:

TABLE II. Genuine scores for combined fingerprint Vs Individual fingerprint.

Combined Template	Individual Fingerprint	Match Score
1 and 2	1	198
1 and 2	2	338
3 and 5	3	398
3 and 5	5	309
4 and 6	4	498
4 and 6	6	210
7 and 8	7	413
7 and 8	8	459
9 and 10	9	435
9 and 10	10	193

Total around 800 genuine scores were calculated and all the scores are in between the range 198 to 780. Few scores were tabulated in Table I.

6.1.2 Imposter Scores:

TABLE III. Imposter scores of combined fingerprints 1 & 2 Vs other Individual fingerprint.

Combined Template	Individual Fingerprint	Match Score
1 and 2	3	9
	4	8
	5	15
	6	16
	7	16
	8	9
	9	14
	10	11

TABLE IV. Imposter scores for combined fingerprints 3 & 5 Vs other Individual fingerprint.

Combined Template	Individual Fingerprint	Match Score
3 and 5	1	9
	2	19
	4	24
	6	15
	7	9
	8	14
	9	29
	10	9

TABLE V. Imposter scores for combined fingerprints 4 & 6 Vs other Individual fingerprint.

Combined Template	Individual Fingerprint	Match Score
4 and 6	1	16
	2	9
	3	17
	5	20
	7	16
	8	14
	9	23
	10	6

TABLE VI. Imposter scores of combined fingerprints 7 & 8 Vs other Individual fingerprint.

Combined Template	Individual Fingerprint	Match Score
7 and 8	1	10
	2	11
	3	20
	4	18
	5	36
	6	11
	9	18
	10	13

TABLE VII. Imposter scores of combined fingerprints 9 & 10 Vs other Individual fingerprint.

Combined Template	Individual Fingerprint	Match Score
9 and 10	1	13
	2	13
	3	25
	4	30
	5	20
	6	13
	7	17
	8	18

Total around 1500 imposter scores were calculated and all the scores are in between the range 10 to 50. Few scores were tabulated in Table II, III, IV, V VI.

Similarity Score:

The Similarity score is calculated from NIST matcher and it compares fingerprints (query fingerprint and original fingerprint) based on the coordinate positions, phase and quality of the minutiae.

Genuine Score:

Genuine Similarity Score is the similarity score between two genuine fingerprints i.e. (query fingerprint is the person's fingerprint who need access).

Imposter Score:

Imposter Similarity Score is the similarity score between imposter fingerprints and fingerprints in the database, i.e. (query fingerprint is the hacker fingerprint who wants access).

Genuine Score will be very high compared to the imposter score. We can observe this from the table.

Comparing the plot, the genuine score is much higher compared with the imposter score. We observe that the genuine scores are always greater than 190 and the imposter scores are always less than 40.

From the similarity scores of genuine and imposter fingerprints obtained and tabulated in table II, III, IV, V, VI, VI the range of genuine and imposter scores are plotted in the figure 6.1 and figure 6.2 respectively, which basically shows the range of genuine between 190 to 750 and imposters scores between 10 to 50.

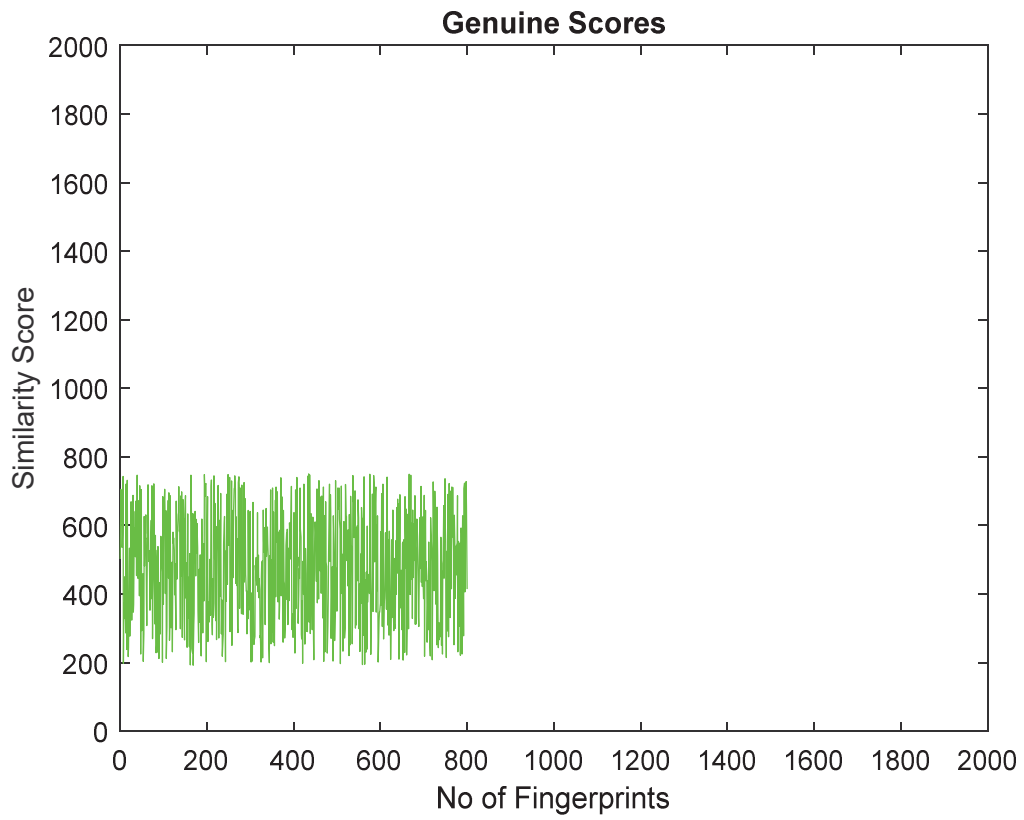


Fig. 6.1: Genuine Scores

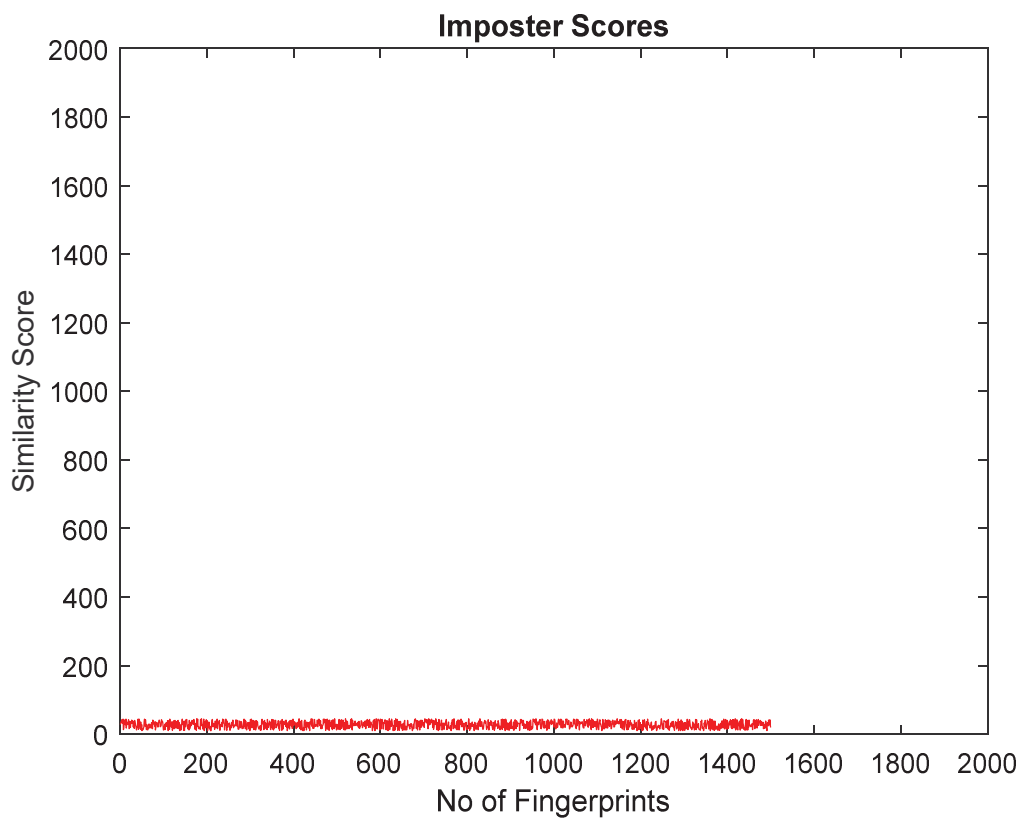


Fig. 6.2: Imposter Scores

Result:

We have combined fingerprints 1 and 2. Let the combined template be A. The score when fingerprint 1 compared with A is 198. The score when fingerprint 2 compared with A is 338, these are genuine scores. The score when fingerprint 3 compared with A is 9. The score when fingerprint 4 compared with A is 8, these are imposter scores since A is formed by combining (1, 2). Therefore, when other fingerprints are compared other than 1 and 2 the scores will be less and the hacker can't pass through the system.

Since we have combined the fingerprints, 2 fingerprints are necessary to access the system. The similarity score must reach as much as in the table in order to access the system.

When there are 2 imposter fingerprints as query fingerprints the scores will not exceed 40 so the system will not give access.

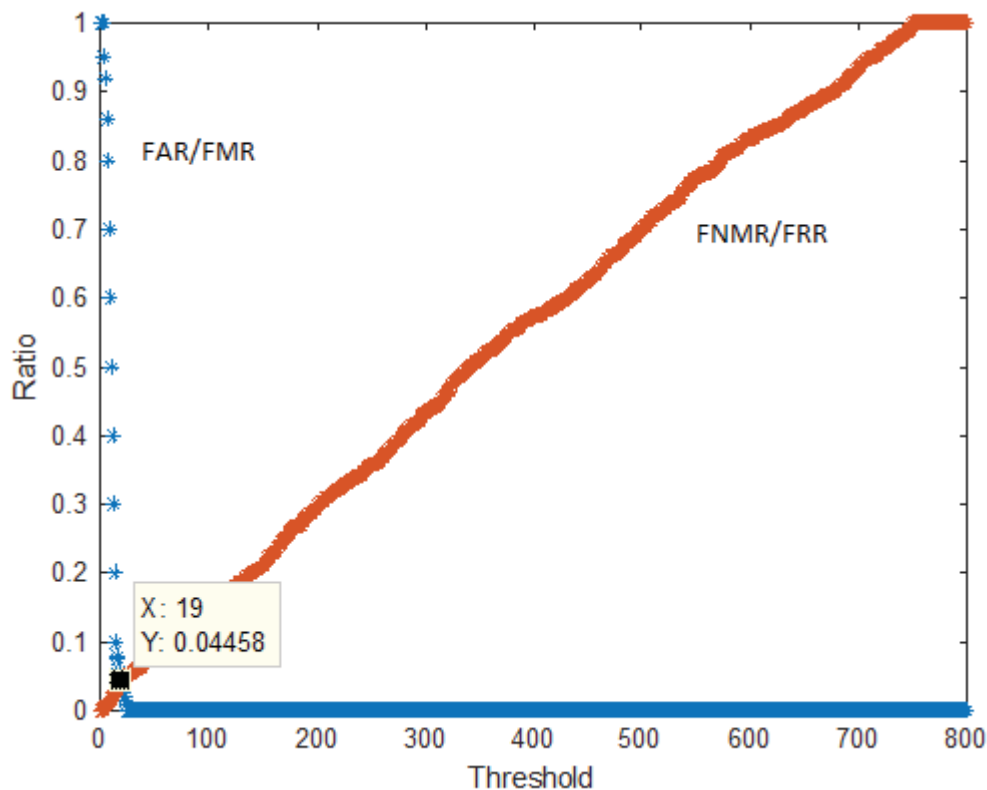


Fig. 6.3: Plot showing EER

EER separates correct users from the imposters. It is the rate at which FMR is equal to FNMR. The performance of the system is also evaluated using EER. EER indicates the accuracy of the system. A single threshold must be chosen to separate the correct user from the imposters.

To know that single threshold we plot both FAR and FRR curves where both intersect at a certain point which is called as EER.

Figure 6.3 is Threshold vs FMR, FNMR, the threshold is taken on x-axis and ratio on y-axis and FMR, FNMR are calculated and plotted with the thresholds. The False Match Rate is 1.0 at very low thresholds since the imposters similarity scores are less. When the threshold increases the imposters are rejected. Hence only genuine fingerprints are accepted, so there are no false matching fingerprints which leads to zero FMR. For FNMR at high thresholds the ratio will be 1.0 because at higher thresholds all the imposter and genuine fingerprints are rejected which indicate all are non-matched. Hence the ratio will be 1.0. At lower thresholds every fingerprint is matched, hence non-match rate is 0.

From the figure 6.3 we can see that Equal Error Rate is 0.044 where the threshold is 19.

6.2 Discussion

6.2.1 Answers to Research Questions

Research Question 1: How does the combination of two fingerprints effect the minutiae position in template?

Answer: Many methods are proposed for fingerprint verification since most years. The combination is done by finding out the minutiae positions, calculating the center of the fingerprint and rotating the image by eigen values, shifting the fingerprint to the origin. The minutiae positions are changed by subtracting the mean value of the fingerprint with the minutiae coordinates.

Research Question 2: How is the proposed algorithm better in terms of similarity score, FMR, FNMR, EER when compared to the existing methods?

Answer: In the previous methods, the similarity calculation was between two fingerprints where the similarity score may be more and the False Acceptance Rate was more. Here since we combine the fingerprints, even though when the data base is stolen the combined fingerprint looks as a single fingerprint, the hacker tries to compare it with the single fingerprint where the score will be less. So here the False Acceptance Rate reduces.

The Equal Error Rate is also reduced when compared with previous methods.

Research Question 3: What is the similarity between original fingerprint and combined fingerprint?

Answer: By observing the similarity scores we find that the scores of single fingerprints are around 40% similar to the combined fingerprint. When the other fingerprint is compared with the combined fingerprint we get scores less than 40.

6.2.1 Problems faced during Implementation

It is imperative, that implementation is done in stages. Attempting to actualize everything on the double will prompt a considerable measure of disarray and confusion.

Another problem faced during implementation is the time taken for the executing the Matlab script. Since the fingerprints data is large and the combination is a lengthy process and also the testing it with single fingerprint became a time-consuming factor.

During the implementation of the system, to get the performance curves the system needs to be tested with the available 50 combined templates. It took more time to compare each fingerprint to compare with each template and for the records.

Chapter 7

Conclusion and Future Work

7.1 Conclusion

We introduce a novel system for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrollment, the system captures two fingerprints from two different fingers. A combined minutiae template containing only a partial minutiae feature of each of the two fingerprints will be generated and stored in a database. To make the combined minutiae template look real as an original minutiae template, we extract features and combine them. In the authentication process, two query fingerprints from the same two fingers are required. Our combined minutiae template has a similar topology to an original minutiae template. Therefore, we can combine two different fingerprints into a new virtual identity by reconstructing a real-look alike combined fingerprint from the combined minutiae template. The experimental results show that our system achieves a very low error rate. It is also difficult for an attacker to break other traditional systems by using the combined minutiae templates. Compared with the state-of-the-art technique, our technique can generate a better new virtual identity (i.e., the combined fingerprint) when the two different fingerprints are randomly chosen. The analysis shows that it is not easy for the attacker to recover the original minutiae templates from a combined minutiae template or a combined fingerprint.

7.2 Future Work

The future work should address the challenges and issues involved in combination and verification and there is always a scope for a new approach which may improve the performance, the future works may involve in exploring new features and new approaches which may be more effective. There is a scope for reducing FAR and EER.

References

- [1] A. Othman and A. Ross, 'Mixing fingerprints for generating virtual identities', in *2011 IEEE International Workshop on Information Forensics and Security*, 2011, pp. 1–6.
- [2] S. Li and A. C. Kot, 'Fingerprint Combination for Privacy Protection', *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 2, pp. 350–360, Feb. 2013.
- [3] Y. Tang, L. Jiang, Y. Hou, and R. Wang, 'Contactless Fingerprint Image Enhancement Algorithm Based on Hessian Matrix and STFT', in *2017 2nd International Conference on Multimedia and Image Processing (ICMIP)*, 2017, pp. 156–160.
- [4] S. Yoon, J. Feng, and A. K. Jain, 'Latent fingerprint enhancement via robust orientation field estimation', in *2011 International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–8.
- [5] M. Wen, Y. Liang, Q. Pan, and H. Zhang, 'A Gabor filter based fingerprint enhancement algorithm in wavelet domain', in *IEEE International Symposium on Communications and Information Technology, 2005. ISCIT 2005.*, 2005, vol. 2, pp. 1468–1471.
- [6] P. B. Patil and N. N. Patil, 'Fingerprint combination using extraction of minutiae position and orientation', in *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, 2016, pp. 1–6.
- [7] R. Nachar, E. Inaty, P. J. Bonnin, and Y. Alayli, 'Minutiae and corner detection in fingerprints without image enhancement for real time recognition', in *2017 8th International Conference on Information, Intelligence, Systems Applications (IISA)*, 2017, pp. 1–6.
- [8] 'History of Fingerprints'. [Online]. Available: http://www.crimescene-forensics.com/History_of_Fingerprints.html. [Accessed: 27-Sep-2018].
- [9] 'An Enhanced Authentication System Using Face and Fingerprint Technologies | Request PDF'. [Online]. Available: https://www.researchgate.net/publication/289175623_An_Enhanced_Authentication_System_Using_Face_and_Fingerprint_Technologies. [Accessed: 27-Sep-2018].
- [10] fslweb, 'Fingerprint Identification', *Forensic Science & Law*, 29-Aug-2016. .
- [11] 'Fingerprinting Part 3-Galton Details - ppt download'. [Online]. Available: <https://slideplayer.com/slide/4736850/>. [Accessed: 27-Sep-2018].
- [12] 'How Fingerprint Scanners Work', *HowStuffWorks*, 24-Sep-2002. [Online]. Available: <https://computer.howstuffworks.com/fingerprint-scanner.htm>. [Accessed: 27-Sep-2018].
- [13] 'FVC2002 - Second International Fingerprint Verification Competition'. [Online]. Available: <http://bias.csr.unibo.it/fvc2002/databases.asp>. [Accessed: 27-Sep-2018].
- [14] J. Ström Bartunek, 'FINGERPRINT IMAGE ENHANCEMENT, SEGMENTATION AND MINUTIAE DETECTION', *DIVA*, 2016.
- [15] T. Nakamura, M. Hirooka, H. Fujiwara, and K. Sumi, 'Fingerprint image enhancement using a parallel ridge filter', in *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.*, 2004, vol. 1, p. 536–539 Vol.1.
- [16] 'Image Processing'. [Online]. Available: http://www.sci.utah.edu/~acoste/uou/Image/project1/Arthur_COSTE_Project_1_report.html#eqhistfunction. [Accessed: 27-Sep-2018].
- [17] 'Histogram equalization', *Wikipedia*. 18-May-2018.
- [18] 'Adaptive histogram equalization', *Wikipedia*. 20-Feb-2018.
- [19] 'EBSCOhost | 87614170 | An Approach to Fingerprint Image Pre-Processing.' [Online]. Available: <http://eds.b.ebscohost.com.miman.bib.bth.se/abstract?site=eds&scope=site&jrnl=20749074&AN=87614170&h=86Zl02Eplxz1RWLP8uYqvCG3ihQShHyszk%2f6XiTCkvO0jU6T%2foOBaMxyBIQHpXswcQmE1z54DyM9rMcNUvvNNg%3d%3d&crl=c&resultLocal=>

- ErrCrlNoResults&resultNs=Ehost&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d20749074%26AN%3d87614170. [Accessed: 27-Sep-2018].
- [20] L. B.N, K. B. Raja, V. K.R, and L. M. Patnaik, ‘Minutiae Extraction in Fingerprint Using Gabor Filter Enhancement’, in *2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies*, 2009, pp. 54–56.
- [21] J. S. Bartunek, M. Nilsson, J. Nordberg, and I. Claesson, ‘Improved Adaptive Fingerprint Binarization’, in *2008 Congress on Image and Signal Processing*, 2008, vol. 5, pp. 756–760.
- [22] ‘Create a Binary Mask - MATLAB & Simulink’. [Online]. Available: <https://www.mathworks.com/help/images/create-binary-mask-from-grayscale-image.html>. [Accessed: 26-Sep-2018].
- [23] ‘Convex Hull — skimage v0.15.dev0 docs’. [Online]. Available: http://scikit-image.org/docs/dev/auto_examples/edges/plot_convex_hull.html. [Accessed: 27-Sep-2018].
- [24] ‘Generate convex hull image from binary image - MATLAB bwconvhull’. [Online]. Available: <https://www.mathworks.com/help/images/ref/bwconvhull.html>. [Accessed: 27-Sep-2018].
- [25] ‘Eigenvalues and eigenvectors’, *Wikipedia*. 18-Sep-2018.
- [26] ‘Four-quadrant inverse tangent - MATLAB atan2’. [Online]. Available: <https://www.mathworks.com/help/matlab/ref/atan2.html>. [Accessed: 27-Sep-2018].
- [27] P. A. Flanagan, ‘NIST Biometric Image Software (NBIS)’, *NIST*, 10-Feb-2010. [Online]. Available: <https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis>. [Accessed: 27-Sep-2018].
- [28] K. Ko, ‘Users Guide to Export Controlled Distribution of NIST Biometric Image Software (NBIS-EC)’, *NIST InteragencyInternal Rep. NISTIR - 7391*, Jul. 2007.
- [29] ‘Minutiae Extraction Based on Propriety of Curvature | Request PDF’, *ResearchGate*. [Online]. Available: https://www.researchgate.net/publication/269801825_Minutiae_Extraction_Based_on_Propriety_of_Curvature. [Accessed: 27-Sep-2018].
- [30] K. Ko, ‘User’s Guide to NIST Biometric Image Software (NBIS) | NIST’, *NIST InteragencyInternal Rep. NISTIR - 7392*, Jan. 2007.
- [31] J. Feng, A. K. Jain, and K. Nandakumar, ‘Fingerprint Matching’, *Computer*, vol. 43, no. 2, pp. 36–44, 2010.
- [32] ‘authentication - Determining the accuracy of a biometric system’, *Information Security Stack Exchange*. [Online]. Available: <https://security.stackexchange.com/questions/57589/determining-the-accuracy-of-a-biometric-system>. [Accessed: 27-Sep-2018].
- [33] ‘An evaluation of preprocessing of noisy fingerprint images by Cellular Frequency Amplification’. [Online]. Available: <http://muep.mau.se/handle/2043/8288>. [Accessed: 27-Sep-2018].