Dedicated to my parents
and all of my honorable teachers

Acknowledgment

Prima facia, I am grateful to the God for the good health and wellbeing that were necessary to complete this thesis. Then I would like to thanks my supervisor Md. Akkas Ali (Assistant Professor) for his enormous support, valuable advice and positive encouragement throughout the course of my thesis. I am grateful to him for his kind assistance, advice and friendly support during my hard work. I also thank my parents for the unceasing encouragement, support and attention.I would like to express my heartfelt thanks to all of you for being with me with immense support and care and to make this work success.

Arun Biswas

December, 2016

Abstract

A fingerprint is an impression of the ridges on the skin of a finger. A fingerprint recognition system uses the distinctive and persistent characteristics from the ridges, also referred to as fingerprint features, to distinguish one finger (or person) from another. Fingerprint recognition system is the best way in the bio-identification applications. There are various types of applications for fingerprint recognition which is used for different purposes. It is used for the purpose of criminal investigation, terrorist identification and security issues. This system consists of many stages like image pre-processing, feature extraction, create template, save template in database and feature match. In pre-processing ,image is enhanced with Gabor filter and heap algorithm is use for matching .The program is coded by using the java. For this system some methods at coding to improve the performance of the recognition system.

Table of Contents

List of Figures

List of Tables

List of Algorithms

Chapter 1

Introduction

1.1 Introduction

A biometric system is an automatic method of identifying a person based on the persons unique physical or behavioural traits, such as a fingerprint or an iris pattern, or a handwritten signature or voice. Biometric identifiers are universal, distinctive, persistent (sufficiently unchangeable over time) and collectable. Biometric systems have become an essential component of effective person recognition solutions because biometric identifiers cannot be shared or misplaced and they naturally represent an individuals bodily identity.

Figure 1.1: Fingerprint

Substitute forms of identity, such as passwords (commonly used in logical access control) and identity cards (frequently used for physical access control), do not provide this level of authentication that strongly validates the link to the actual authorized user. Fingerprint recognition is the most popular and mature biometric system used today. In addition to meeting the four criteria above, fingerprint recog-

nition systems perform well (that is, they are accurate, fast, and robust), they are publicly acceptable, and they are hard to circumvent.

A fingerprint is an impression of the ridges on the skin of a finger. A fingerprint recognition system uses the distinctive and persistent characteristics from the ridges, also referred to as fingerprint features, to distinguish one finger (or person) from another .It is the combination of both ridges and furrows.

Finger prints can be distinguished by using the minutiae; these are nothing but some abnormal points on the ridges. Minutiae consist of two main parts such as: termination and bifurcation. Termination is the point where your ridge ends and bifurcation is the point where ridge divides into branch again minutiae having both ridges and furrows. Valley is also a furrow.

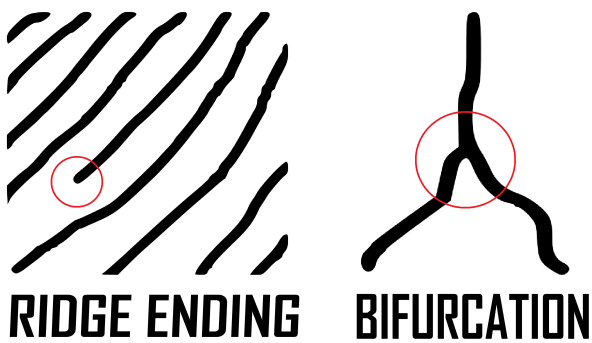

Figure 1.2: Minutiae.

The fingerprint recognition problem having two methods: fingerprint verification and other is fingerprint identification. The fingerprint recognition is called as AFRS (Automatic Fingerprint Recognition System), which is program-based. However, in all fingerprint recognition problems, either verification(one to one matching)

or identification(one to many matching), the underlining principles of well-defined representation of a fingerprint and matching remains the same.

1.2 Background and Present State

There are many benefits of using biometrics as an authentication tool over traditional knowledgebased or token-based tools that includes increased security, increased convenience, reduced fraud or delivery of enhanced services. Access to personal computers, networks and applications, access to secured areas of a building, authorisation at automatic teller machine (ATM) and transaction in online banking are some common applications of knowledge-based autehtication systems. Handheld tokens such as cards and key fobs are used mainly for building access but they have replaced passwords in some high security applications. The generation of personal identification number (PIN)s using key generator for online banking is an example of this. However, passwords, PINs, tokens or cards have a number of weaknesses that may raise concern about their suitability in modern applications, especially high-security applications such as acess to online financial accounts or medical data. The authentication mechanism can be implemented by any of the followings or combination of these:-

- Something you know such as passwords and PINs.
- Something you have such as smart cards, keys or tokens.
- Something you are, which refers to biometrics- the measurement of physical characteristics or personal traits.

The knowledge based system which is based on passwords and PINs is still most widely used authentication system but the shortcomings of the knowledge-based or token based authentication can be overcome by the introduction of biometrics and the benefits it can bring are

- **Increased Security:** Biometrcis can provide an enhanced level of security to the traditional authentication methods by allowing access only to authorised users and restrict access or protect data from unautorised users. Although password is meant to be confidential, should be hard to guess and should not be written down; in practice, people often forgot their passwords, sometimes share it with their friends and colleagues. Many users use obvious words or numbers to make passwords and PINs that can be easily guessed so unauthorised users can break into account with little effort. Good passwords , i.e. long passwords with numbers and symbols, are difficult to remembr for most users and rarely enforced. On the other hand, biometric data cannot be guessed or stolen in the same way as password or token. Although some biometric systems can be broken under certain conditions, todays biometric systems are highly unlikely to be fooled by a picture of a face, an impression of a fingerprint or recording of a voice. This assumes, of course, that the imposter has been able to gather these physiological characteristic- which is unlikely in most cases.

- **Increased convenience:** Most of the time, ordinary users choose simple words as their passwords so they are not forgotten. As computer users are forced to manage a number of passwords, the likely hood of passwords being forgotten increases unless the user choose to use a universal password for every login, which in effect reduces the security. Tokens and cards can sometimes be forgotten or lost. Because biometrics are always attached with the person and so there is nothing to forgot. It offers a greater convenience than systems based on remembering multiple passwords or on keeping possession of an authentication token. For PC applications, where users can have access to multiple resources, biometric can simplify the authentication process by replacing multiple passwords and thus reduce the burden on both the user and the system administrator. Applications such as point of sale transactions have also begun to see the use of biometrics to authorise purchases from prefunded accounts, eliminating the need for cards. Biometric authentication can also

be used to allow users to access higher level of rights and privileges. Highly sensitive and critical information can be readily available on a biometrically protected network than on one protected by passwords. This can increase user and enterprise conveniences, as users can access otherwise protected information without the need for human intervention.

- **Increased accountability:**The increased awareness of security in the enterprise and service industry has put a huge demand on auditing and reporting capabilities. Biometrics can be a very useful tool to secure computers and facilities and offer a high degree of certainity as to what an user has accessed in which computer at what time. Although the auditing and reporting capability of a computer system is rarely used, the presence of such system can be an effective deterrent for fraudsters. Until now, a number of biometric technologies has been developed and deployed in different industries and some are still in the development process. Each biometric technology has its own advantages and disadvantages but they should be considered and evaluated giving full consideration to the following characteristics:

  - Universality: Every person should have the characteristic. People who are mute or does not have a fingerprint will need to be accommodated in some way.
  - Uniqueness: Generally, no two people have identical characteristics. However, identical twins are hard to distinguish.
  - Permanence: The characteristics should not vary with time. A person's face, for example, may change with age.
  - Collect-ability :The characteristics must be easily collectible and measurable.
  - Performance: The method must deliver accurate results under varied environmental circumstances.

– Acceptability: The general public must accept the sample collection routines. Nonintrusive methods are more acceptable.

– Circumvention: The technology should be difficult to deceive.

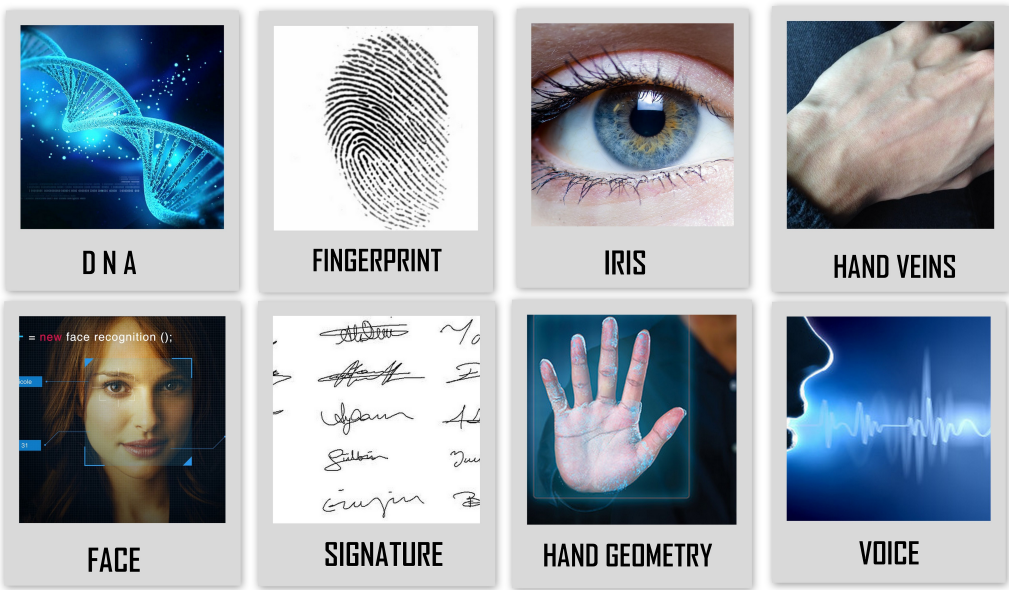

Figure 1.3: Different Biometric features that can be used to generate uniqueness

Some biometric features that can be used to generate uniqueness for a person are shown in Figure 1.3. Not all of them have gained the same level of acceptance in the industry due to their cost and viability in deployment.

Among all biometrics, fingerprint biometrics has proved itself the most promising and cost-effective solution in security systems. Its lower cost and accuracy has brought itself in the leading position of all biometric solutions as can be seen from Figure 1.4. Although other biometric technologies are gaining popularity, fingerprint is likely to maintain its leading position in the near future. At present, nearly half of the biometric solutions are being implemented using fingerprint biometrics [1].

In recent years, government and commercial organizations have substantially increased their own deployment of fingerprint based recognition systems in non

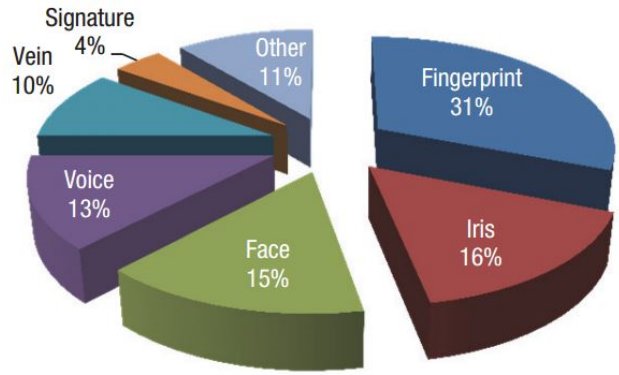

Figure 1.4: Global Biometric Market Projections

forensic applications, including physical and logical access control due to rising concerns about security and fraud. Automatic fingerprint recognition systems performs reliably well as far as recognition is concerned [2].Over the last two decades, research in fingerprint recognition has seen tremendous growth. Several automatic fingerprint identification systems (AFIS) have been developed for civil, military and forensic applications. FBI-AFIS, US border security and EU passport/ID system are few examples of large scale applications of fingerprint biometrics [1].

The main reasons for the popularity of fingerprint recognition are [1]

- Its success in various applications in the forensic, government, and civilian domains.
- The fact that criminals often leave their fingerprint at crime scenes.
- The existence of large legacy databases and
- The availability of compact and relatively inexpensive fingerprint readers.

Although significant progress has been made in automatic fingerprint identification in recent years, there are still a number of issues that need to be addressed to improve systems performance and accuracy.

1.3 Motivation and Aims

Biometrics-based security, such as fingerprint authentication, is proven to be both more secure and convenient than passwords, making fingerprint sensing an increasingly common – and product-differentiating – feature in smart phones, tablets and PCs. However, fingerprint authentication also raises security concerns that can best be addressed with protections purpose-built for biometrics. Synaptic helps ensure biometric data protection through the Sentry Point Security Suite of features and architectures that accommodate the full range of market needs .So for a better security we need fingerprint based authentication system. We need to keep faster and better performance from the system. The performance depends upon the quality of images and the size of template. So our main work is capture the fingerprint image and create a better quality of fingerprint template and it converted into a byte stream and keep in a database.

1.4 Objectives and Specific Aims

The main Objectives and Specific Aims is :

- To increase the image quality .
- Verification and Identification.
- To establish a better security system.
- To get a better accuracy .
- To keep data in database as byte stream .

1.5 Organization of the Thesis

The dissertation is organized as follows:

- **Chapter 1 Introduction.** In this chapter an introduction to the fingerprint recognition system has been given.
- **Chapter 2 Literature Review.** This chapter shows the state of the art work in the field of fingerprint recognition system.
- **Chapter 3 Methodology.** We present our proposed technique to recognize fingerprint in this chapter.
- **Chapter 4 Experimental Analysis.** In this chapter, it has been shown the effectiveness and efficiency of our proposed model.
- **Chapter 5 Conclusions and Future Work .** Finally, this chapter concludes the dissertation indicating the limitations and future works.

Chapter 2

Literature Review

This section provides a brief literature survey of the fingerprint matching system. The fingerprint matching can be achieved using minutiae, correlation and pattern [3].David [1] proposed a fingerprint matching based on the graph-matching algorithm using graduated assignment.Jain, Ross and Prabhakar [4] proposed a hybrid fingerprint matching algorithm which used both minutiae points and texture information in local region.Gabriel, Oluwole and Olumuyiwa [5] proposed a fingerprint matching based on the correlation coefficiency using distance feature from core to minutiae.Subhas et. al. [2] proposed a fingerprint matching based on spatial information (distance) of minutiae point only and used indexing technique to speed up the matching process.Feng, Ouyang and Cai [6] proposed a fingerprint matching based on both ridge and minutiae correspondences. The N initial substructures found in the novel alignment (adjacent ridge and minutiae) are used for fingerprint matching.Andrej, Alexej and Justas [7] proposed minutiae based fingerprint matching algorithm using local structure. The characteristic in the local structure are: rotation and translation invariance, locality (for tolerance to deformations) and fast and easy comparable.Ito, Nakajima, Kobayashi, Aoki and Higuchi [8], proposed a fingerprint matching system using phase-only correlation which is invariant to shift, brightness and noise.Ning, Yilong and Hongwei [9] proposed a fingerprint matching algorithm based on Delaunay Triangulation in which co-ordinates and orientation of the minutiae point are used. The algorithim is even applicable for finger print images of different resolutions.Asker and Sabih [10]

proposed elastic minutiae matching algorithm using non-linear transformation model. The non-linear transformation model consists of two stages: first is local matching based on local similarity measurement and the second is global matching which uses the possible correspondences to estimate a global non-rigid transformation.Karthik [11] proposed a fingerprint matching algorithm based on two stage i.e. local phase spectra and global phase spectra. The final matching decision is based on the fusion of both the global and local similarity score.Xifeng, Jianhua, Xianglong and Daming [12] proposed fingerprint minutiae matching using the adjacent feature vector. The Adjacent Feature Vector (AFV) consists of four adjacent relative orientations and six ridge count of a minutiae. Xuejun and Bir [13] proposed a minutiae fingerprint matching based on genetic algorithm. The fitness function which used in genetic algorithm is based on the properties of minutiae which include angles, traingle handedness, traingle direction, maximum side, minutiae density and ridge count.Weiguo, Howells, Fairhurst and Deravi [14] proposed a memetic fingerprint matching algorithm, which aims at identifying the optimal and near optimal minutiae matching using genetic algorithm. Minutiae descriptor containing orientation and circular region around the minutiae point is used as local feature.

Chapter 3

Methodology

3.1 System Implementation

The fingerprint authentication system consists of fingerprint acquiring device as a sensor, minutia extraction and fingerprint matcher. The matching stage is divided into two process that is identification and verification. At the time of capture fingerprint image the pre-processing stage is applied to it. The output of this stage will be passed to feature extraction stage which is extract the minutiae point(ridge ending, Bifurcation) from thinning fingerprint image, then the false minutiae removal is applied to extract real minutiae. After that fingerprint is enrolled and fingerprint template is created and then the work is converted template into byte stream. Finally the byte stream is stored in the MySQL database. If the fingerprint is already enrolled,then it sends to matching stage otherwise go enrollment stage for create template, after this it convert to byte stream and store in the database. In identification case (one-to-many matching), the input feature set which is matching with N template from database, N matching will be done. The result will be consider as matching Score. If matching Score closer to 1 then both fingers from same user. If matching score near to Zero then both fingers from different user. In verification case (one-to-one matching) ,the input feature set which is matching with one template from database, one matching will be done and decided either the input fingerprint verified or unverified.

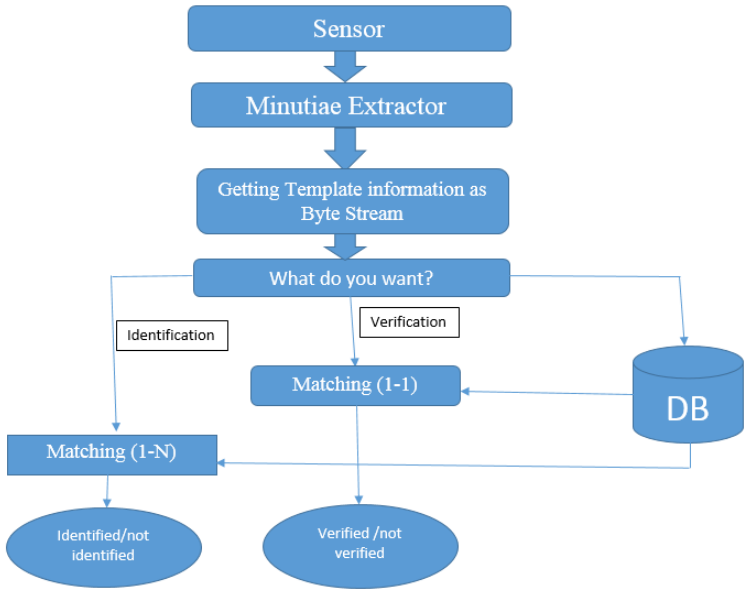

Figure 3.1: Proposed Method

3.2 System level design

3.2.1 Sensors

A fingerprint scanner is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching.

Figure 3.2: Fingerprint sensor

Many technologies have been used including optical, capacitive, RF,thermal, piezoresistive, ultrasonic, piezoelectric, MEMS.It is a type of biometric security technology that utilizes the combination of hardware and software techniques to identify the fingerprint scans of an individual.

3.2.2 Minutiae Extractor

To implement a minutia extractor, a three method is used by researcher.They are pre -processing, minutia extraction and post processing stage.

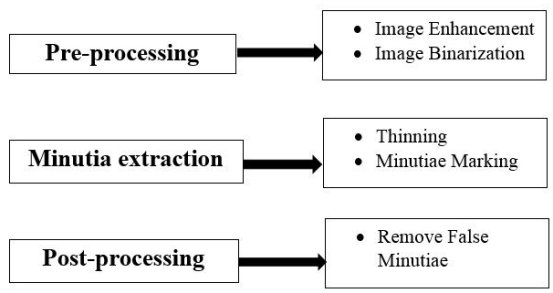

Figure 3.3: Minutiae Extraction

3.2.3 Pre-processing

Pre-processing stage in image processing is one of the most critical stage because the final results of post processing stage are entirely depends on this stage and the reason is quite obvious, because the image that user want to recognize may contains noise or the medium from which it taken, may not gave appropriate or standard quality image. In fingerprint recognition the most important step is accurately extricating finer points from the query finger impression , that which doesn't matters from which channel it was taken or how much noise variation are present, system must process each on every image and show results accurately. In order to make standardized image,

some enhancement techniques are applied, so that the system shall provide best possible results in latter stages.

3.2.3.1 Image Enhancement

Fingerprint image enhancement is used to make image quality more clear for better use. The image enhancement is also used to reduce the noise and to enhance the definition of ridges against valleys. Here we used two methods for image enhancement stage those are:

- **Histogram Equalization:** Histogram equalization is mainly used to increase the pixel value of an image . By using this method we can improve the contrast of an image. The original histogram and having the range from 0 to 255 and also the visualization effect is goes on increasing.

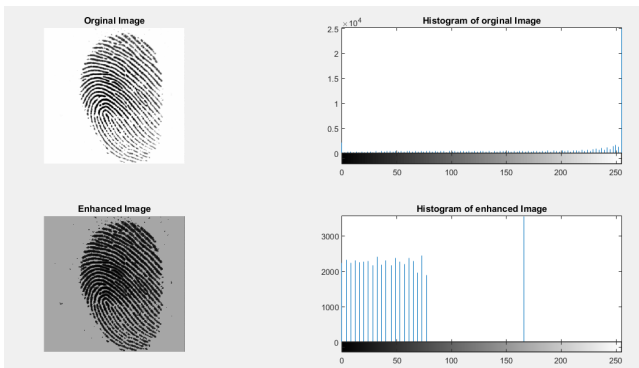

Figure 3.4: Image Enhancement by Histogram Equalization

- **Gabor filtering:**A Gabor filter is used for this process and a suitable value of local variances is taken for carrying out the process of filtering. A Gabor filter takes care of both the frequency components as well as the spatial coordinates. The inputs required to create a Gabor mask are frequency, orientation angle and variances along x and y directions. Filtering is done for each block using the local orientation angle and frequency. Once the ridge orientation and ridge frequency information

has been determined, these parameters are used to construct the even-symmetric Gabor filter. A two dimensional Gabor filter consists of a sinusoidal wave of a particular orientation and frequency, modulated by a Gaussian envelope.

Gabor filters are employed because they have frequency-selective and orientation-selective properties. These properties allow the filter to be tuned to give the best response to ridges at a specific orientation and frequency in the fingerprint image. Therefore, a properly tuned Gabor filter can be used to effectively preserve the ridge structures while reducing noise. The even-symmetric Gabor filter is the real part of the Gabor function.

$G(x, y; \theta, f) = \exp[-\frac{1}{2}[\frac{x_\theta^2}{\alpha_x^2} + \frac{y_\theta^2}{\alpha_y^2}]] \cos(2\Pi f x) - - - - - - - - (1),$

$$x_\theta = x \cos\theta + y \sin\theta$$

,

$$y_\theta = -x \sin\theta + y \cos\theta$$

In equation (1) , θ is the local orientation, f is the frequency, α_x and α_y are the standard deviation of the Gaussian envelope .

The fingerprint image is enhanced by convolving the normalized image with the Gabor filter. The convolution for a pixel requires the pixels corresponding orientation and frequency values, these values are used to construct a Gabor filter specific to that pixel .Thus the convolution will result in the noise being reduced and the ridges being enhanced, since the Gabor filter only filters along the specified orientation, it decreases anything oriented differently. Hence, the filter increases the contrast and reduces the noise.

Figure 3.5: Image Enhancement by Gabor filtering

3.2.3.2 Image Binarization

Binarisation is the process that converts a grey level image into a binary image. This improves the contrast between the ridges and valleys in a fingerprint image, and consequently facilitates the extraction of minutiae.

Most minutiae extraction algorithms operate on binary images where there are only two levels of interest: the black pixels that represent ridges, and the white pixels that represent valleys.

Fingerprint Image binarization transforms the 8-bit Gray fingerprint image to a 1-assigned for ridges and 0 assigned for furrows. After these operations, the ridges in the fingerprint will be highlighted with black color while furrows will be color with white.

Process of binarization is-

- calculate the average of rgb color values from a cell;
- if(average > 127) then the cell is 1;
- else cell is 0;

Figure 3.6: Image Binarization

3.3 Minutiae Extraction

Minutiae extraction have two steps:

3.3.0.3 Thinning

Image thinning is used to reduce the darkness of all ridge lines. Thinning process does not convert the original location. Ridge thinning is used to destruct the extra pixel of ridges until just one Pixel broad.

Thinning process based on the A Fast Parallel Algorithm for Thinning Digital Patterns by T. Y. Zhang & C.Y. Suen, for each center point P1, it's neighboring cells will be defined in Figure 3.7.

P9 (i-1,j-1)	P2 (i-1,j)	P3 (i-1,j+1)
P8 (i,j-1)	P1 (i,j)	P4 (i,j+1)
P7 (i+1,j-1)	P6 (i+1,j)	P5 (i+1,j+1)

Figure 3.7: Thinning process

We go through all center cells and see which cells to re-color as Black/1 based on these conditions:

- $3 <= B = P2 + P3 + P4 + P5 + P6 + P7 + P8 + P9 <= 6$
- A(P1)= 1; center point must be Black/1 itself!
- if($A == 1 \&\& 3 <= B <= 6$) then center cell color is black/1
- else color is white/0

Figure 3.8: Thinning Image

3.3.0.4 Minutiae Marking

The concept of Crossing Number (CN) is widely used for extracting the minutiae [2, 4, 5, 15] . Rutovitzs definition [9] of crossing number for a pixel P is

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Figure 3.9: Crossing Number

$$CN = \frac{1}{2}\sum_{i=1}^{8}(\lceil P_i - P_{i+1} \rceil) - - - - - - - - - - (2)$$

Where Pi is the binary pixel value in the neighbourhood of P with

$$P_i = (0 \quad \text{or} \quad 1) \quad \text{and} \quad P_1 = P_8,$$

The skeleton image of fingerprint is scanned and all the minutiae are detected using the properties of CN, CN has 5 properties and they are -

- If CN =0 then it is Isolated point
- If CN=1 then it is Ending point
- If CN=2 then it is Connective point
- If CN=3 then Bifurcation point
- If CN=4 then Crossing point

and its illustration is

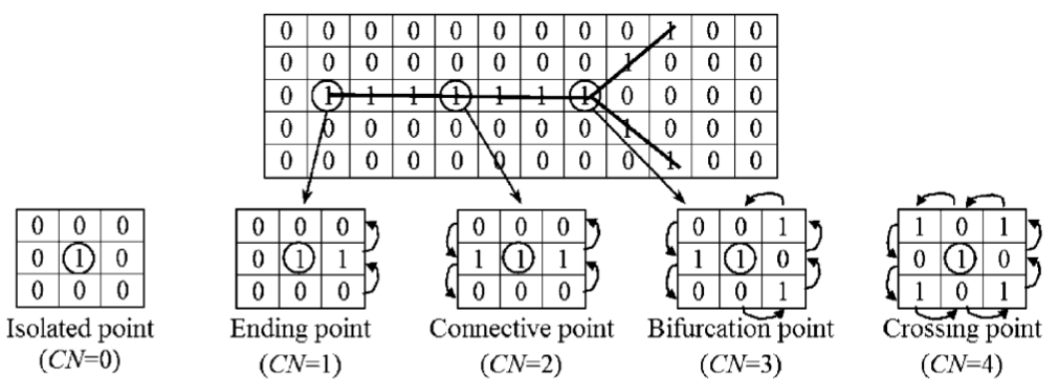

Figure 3.10: Crossing Number process

3.3.0.5 Post-processing

In order to eliminate false minutiae, we have chosen to implement the minutiae validation algorithm. This algorithm tests the validity of each minutiae point by scanning the skeleton image and examining the local neighbourhood around the point.

P9 (i-1,j-1)	P2 (i-1,j)	P3 (i-1,j+1)
P8 (i,j-1)	P1 (i,j)	P4 (i,j+1)
P7 (i+1,j-1)	P6 (i+1,j)	P5 (i+1,j+1)

Figure 3.11: Post-processing

- if($P2 * P4 * P6 = 0$) then center cell 1
- if($P2 * P6 * P8 = 0$) then center cell 1
- otherwise cell is 0

The first step in the algorithm is to create an image M of size $W \times W$, where M corresponds to the $W \times W$ neighbourhood centred on the candidate minutiae point in the skeleton image. The central pixel of M corresponds to the minutiae point in the skeleton image, and so this pixel is labelled with a value of 1. The rest of the pixels in M are initialized to values of zero, as shown in Figure 3.10(a) and Figure 3.11(a). The subsequent steps of the algorithm depend on whether the candidate minutiae point is a ridge ending or a bifurcation.

a) For a candidate ridge ending point:

1. Firstly, label with a value of 1 all the pixels in M , which are eight-connected with the ridge ending point (see Figure 3.10(b)).

2. The next step is to count in a clockwise direction, the number of 0 to 1 transitions (P_1) along the border of image M . If P_1= 1,then the candidate minutiae point is validated as true ridge ending.

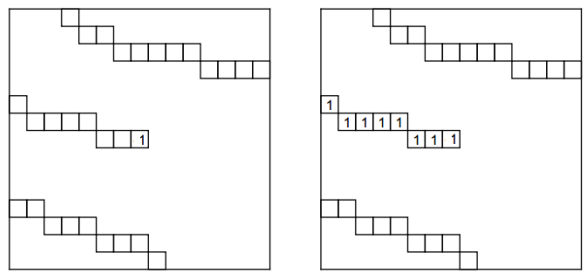

Figure 3.12: ridge ending point

b) For a candidate bifurcation point:

1. Firstly, examine the eight neighbouring pixels surrounding the bifurcation point in a clockwise direction. For the three pixels that are connected with the bifurcation point, label them with the values of 1, 2, and 3, respectively. An example of this initial labelling process is shown in Figure 3.11(b).

2. The next step is to label the rest of the ridge pixels that are connected to these three connected pixels. This labelling is similar to the ridge ending approach, however, instead of labelling a single ridge branch, three ridge branches are now labelled. Let l = 1, 2 and 3 represent the label for each ridge branch. For each l, label with l all the ridge pixels that have a label of 0, and connected to an l labelled pixel. Examples of the bifurcation labelling process are shown in Figures 3.11(c), (d) and (e).

3. The last step is to count in a clockwise direction, the number of transitions from 0 to 1 (P_1), 0 to 2 (P_3), and 0 to 3 (P_5) along the border of image M . If $P_1 = 1$,$P_3 = 1$ and $P_5 = 1$,then the candidate minutiae point is

validated as a true bifurcation.

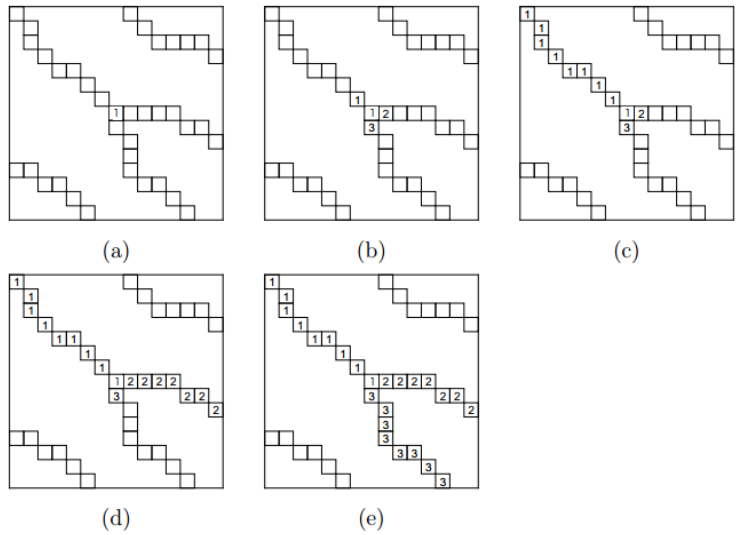

Figure 3.13: bifurcation point

3.3.1 Getting information from Fingerprint using Heap algorithm

The heap-based Fingerprint Matching algorithm is based on heap tree property. This algorithm is very simple, yet robust and powerful. Let I_a be a 2D fingerprint image with a main point . Let M^a_{ij} be the minutiae point of Image I_a, where i is number of minutiae points and j=1,2,3,4. A row comprises of four points $< d^a_{i1}, X^a_{i2}, Y^a_{i3}, b^a_{i4} >$ where d_i is the distance of i^{th} minutiae point from main point (X^a_m, Y^a_m) and it is calculated using Euclidean distance, i.e.,

$$d^a_i = \sqrt{(x^a_i - x^a_m)^2 + (y^a_i - y^a_m)^2}$$

(X^a_i, Y^a_j) is the coordination of i^{th} minutiae point and b^a_i is Boolean value of minutiae i.e. either ridge ending or ridge bifurcation. The H_a is a MinHeap for M^a_{ij} with respect to the distance d^a_i from main point (X^a_m, Y^a_m).

Algorithm 1: Getting information using Heap algorithm

H_a is a Min-Heap of image I_a.;

I_a is a preprocessed image of fingerprint;

The minutiae points of I_a are calculated and stored in M_{ij}^a ;

$distance(d_a) \leftarrow H_a$;

for $i = 1$ *to* n **do**

  $d_i^a = \sqrt{(x_i^a - x_m^a)^2 + (y_i^a - y_m^a)^2}$;

  for $i = 1$ *to* 4 **do**

    $M_{i,j}^a = [d_{i,1}^a, X_{i,2}^a, Y_{i,3}^a, b_{i,4}^a]$;

  end

end

H_a = BuildMin-Heap M_{ij}^a ;

The construction of minimum Heap is the main task of the proposed algorithm. In this construction, minutiae is detected and the distance between two minutiae points are calculated. Using the distances, d, minimum heap is constructed where N1, N2,..... are the nodes. Nodes are represents the minutia points of fingerprint image.

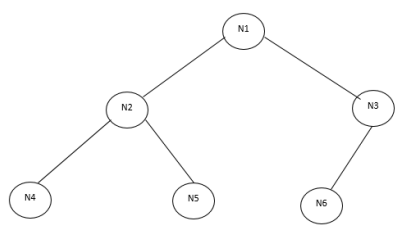

Figure 3.14: Minimum Heap from minutiae points

Minimum Heap re-presents the total information of minutiae .And we keep this information in database as a byte stream for verification and identification.

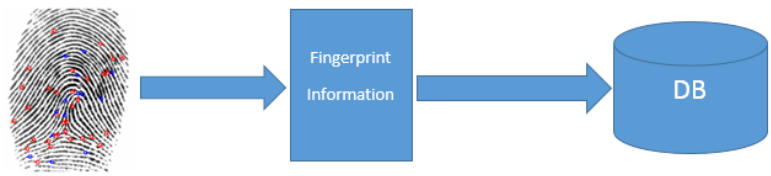

Figure 3.15: Keeping information in database

3.3.2 Fingerprint Matching using Heap algorithm

Let us consider two MinHeap H_a and H_b and compare the top and delete it as shown in the Algorithm. This algorithm takes a main point of the images and calculates the distances. This algorithm constructs H_a and H_b based on the distance of every minutiae point from the main point (X_m^a, Y_m^a) and (X_m^b, Y_m^b) respectively.

Algorithm 2: Fingerprint Matching using Heap algorithm

```
Compare(H_a, H_b);
Initialize the working variables:;
distance(d_a) ← H_a;
distance(d_b) ← H_b;
while H_a&&H_b ≠ empty do
    currentBest ← −1;
    for i ← 0; i < H_b.length; i++ do
        if d_a == d_b then
            currentBest=1;
        end
    end
    if Type of minutia is same then
        Hit=hit+1;
        Add next node;
    else
        missing++;
        Add next node;
    end
end
```

After applying the above algorithm, a hit value is determined which gives the number of matching minutiae. Using these hit values, an accuracy is calculated to determine the matching parameter . A robust orientation-independent fingerprint matching technique and the equation is

$Accuracy = \frac{Hit}{N}$

N=Number of nodes in H_a or H_b which ever is minimum ;

Chapter 4

Experimental Analysis

The experiment is performed by using Java, matlab and tested on databases MySQL . Finally we get result from pre-processing stage matching stage, database stage , identification (one to-many)matching, verification system(one-to-one)matching and accuracy .

4.1 False Rejection Rate (FRR)

Sometimes the biometric security system may incorrectly reject an access attempt by an authorized user. To measure these types of incidents FRR is basically used. A systems FRR basically states the ratio between the number of false rejections and the number of identification attempts.

$$(\%)FRR = \frac{FR}{N} * 100$$

FR=number of missing nodes. N= number of samples or Number of nodes.

And the average FRR is 0.0047

4.2 False Acceptance Rate (FAR)

Sometimes the biometric security system may incorrectly accept an access attempt of an unauthorized user. To measure these types of incidents FAR is basically used.

A systems FAR basically states the ratio between the number of false acceptances and the number of identification attempts.

$$(\%)FAR = \frac{FA}{N} * 100$$

FA = number of accepted nodes. N =total number of samples or Number of nodes.

And the average FAR is 0.0173

4.3 Gabor filter enhancement

Fingerprint Identification System (FIS) is very commonly used in the bio-identification applications. This Project finds out the current techniques for fingerprint recognition. The performance depends upon the quality of images .For this we use gabor filter for enhancement .And get better performance then fft enhancement in fig 4.1.

Figure 4.1: FFT enhancement and Gabor filter enhancement

4.4 Byte String

Byte string is better then blob for fingerprint authentication system.

Table 4.1: Difference of data-type

Data-type	Size
Blob	64k
byte stream	4k

Blob's max size is 64Kb where byte string is 4Kb. If fingerprint database size is 64 Kb and we use byte string then we can keep 14 to 15 templates in database where blob's size is 64 Kb. So for a small template, a byte string is better solution .

4.5 Identification(1-N)

It is the process for comparing between the user of biometric data and multiple users of template data which take at enrollment phase. In this process the similarity between input and all users in template database is found. The Identification process is also known as(1:N)matching. It is performed when the user provides his/her biometric data and performed the multiple comparisons from number of users to find the matching. The result will be users fingerprint is identified or not identified.

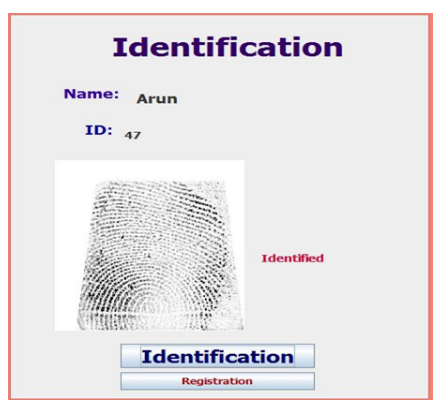

Figure 4.2: Identification

4.6 Verification(1-1)

It is the process of comparison between the user of biometric data and one template. The Verification contain various of biometric data recorded but one of biometric data is matched. This process also is known as (1:1) matching. The result will be found or not found.

Figure 4.3: Verification

4.7 Accuracy

The proposed system is compared with previous fingerprint recognition system and the result is

Table 4.2: Accuracy table.

Reference	Accuracy	Year
[10]	98.02%	2009
[16]	98.55%	2016
[17]	98.6971%	2016
[18]	98.56%	2016
proposed method	99%	2016

Proposed system accuracy is 99% which is better than past accuracy.

Chapter 5

Conclusions and Future Work

In this chapter we summarize the research works presented in this dissertation and make final concluding remarks with few directions for future works.

5.1 Conclusion

The Heap based fingerprint algorithm can revolutionize the fingerprint orientation-independent algorithm which is simple but powerful than the orientation based fingerprint matching algorithm as it can match in many possible angle of a fingerprint image. The proposed system uses minimum feature i.e. distance and type of minutiae for matching so it can be used for online verification system.

The work is done in sequence start from the first stage which is pre-processing which is used to remove unwanted data and increased the clarity of ridges of fingerprint image. The second step is the feature extraction which is used to extract the fingerprint features. In this work we focus on ridge ending and bifurcation which is done by using minutiae extractor algorithm .The third step of this work is the matching which is divided into two parts identification process also known as(1:N)matching or verification process also known as(1:1 matching). We used real life fingerprint data from users and keep it in database in secured process.

5.2 Future work

The future work is to do fingerprint identification and verification by using neural network and fuzzy logic in order to enhance and evaluate the best performance of fingerprint recognition system.

Bibliography

[1] D. A. Braude, "Fingerprinnts: oriantation free minutiae extraction and using distances between minutiae for identification and verification," Ph.D. dissertation, 2011.

[2] S. Barman, S. Chattopadhyay, D. Samanta, S. Bag, and G. Show, "An efficient fingerprint matching approach based on minutiae to minutiae distance using indexing with effectively lower time complexity," in *Information Technology (ICIT), 2014 International Conference on.* IEEE, 2014, pp. 179–183.

[3] A. Chandrasekaran and B. Thuraisingham, "Fingerprint matching algorithm based on tree comparison using ratios of relational distances," in *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on.* IEEE, 2007, pp. 273–280.

[4] A. Jain, A. Ross, and S. Prabhakar, "Fingerprint matching using minutiae and texture features," in *Image Processing, 2001. Proceedings. 2001 International Conference on*, vol. 3. IEEE, 2001, pp. 282–285.

[5] G. B. Iwasokun, O. C. Akinyokun, and O. J. Dehinbo, "Minutiae interdistance measure for fingerprint matching." Intl Conference on Advanced Computational Technologies & Creative Media (ICACTCM2014) Aug, 2014.

[6] J. Feng, Z. Ouyang, and A. Cai, "Fingerprint matching using ridges," *Pattern Recognition*, vol. 39, no. 11, pp. 2131–2140, 2006.

[7] A. Kisel, A. Kochetkov, and J. Kranauskas, "Fingerprint minutiae matching without global alignment using local structures," *Informatica*, vol. 19, no. 1, pp. 31–44, 2008.

[8] H. Nakajima, K. Kobayashi, M. Morikawa, A. Katsumata, K. Ito, T. Aoki, and T. Higuchi, "A fingerprint matching technique based on phase-only correlation," *IEEJ Transactions on Sensors and Micromachines*, vol. 126, pp. 38–46, 2006.

[9] N. Liu, Y. Yin, and H. Zhang, "A fingerprint matching algorithm based on delaunay triangulation net," in *The Fifth International Conference on Computer and Information Technology (CIT'05)*. IEEE, 2005, pp. 591–595.

[10] A. M. Bazen and S. H. Gerez, "Elastic minutiae matching by means of thin-plate spline models," in *Pattern Recognition, 2002. Proceedings. 16th International Conference on*, vol. 2. IEEE, 2002, pp. 985–988.

[11] K. Nandakumar, "Fingerprint matching based on minutiae phase spectrum," in *2012 5th IAPR International Conference on Biometrics (ICB)*. IEEE, 2012, pp. 216–221.

[12] X. Tong, J. Huang, X. Tang, and D. Shi, "Fingerprint minutiae matching using the adjacent feature vector," *Pattern Recognition Letters*, vol. 26, no. 9, pp. 1337–1345, 2005.

[13] X. Tan and B. Bhanu, "Fingerprint matching by genetic algorithms," *Pattern Recognition*, vol. 39, no. 3, pp. 465–477, 2006.

[14] W. Sheng, G. Howells, M. Fairhurst, and F. Deravi, "A memetic fingerprint matching algorithm," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 402–412, 2007.

[15] B. M. Mehtre, "Fingerprint image analysis for automatic identification," *Machine Vision and Applications*, vol. 6, no. 2-3, pp. 124–139, 1993.

[16] M. M. Ali, V. H. Mahale, P. Yannawar, and A. Gaikwad, "Fingerprint recognition for person identification and verification based on minutiae matching," in *Advanced Computing (IACC), 2016 IEEE 6th International Conference on*. IEEE, 2016, pp. 332–339.

[17] V. C. Bjorn and S. J. Belongie, "Fingerprint recognition system," Sep. 26 2000, uS Patent 6,125,192.

[18] C. Sahu and V. Jain, "A novel approach to fractal dimension based fingerprint recognition system," 2016.