Department of Space, Government of India

Indian Institute of Space Science and Technology

Thiruvananthapuram

RS322 – Pattern Recognition

Project Report
on

Minutiae-based Fingerprint Matching

Submitted By:
Nikhil S Hubballi
SC13B158
Physical Sciences

CONTENT:

INTRODUCTION

Personal identification is to associate a particular individual with an identity. It plays a critical role in our society, in which questions related to identity of an individual such as “Is this the person who he or she claims to be?”, “Has this applicant been here before?”, “Should this individual be given access to our system?” “Does this employee have authorization to perform this transaction?” etc. are asked millions of times every day by hundreds of thousands of organizations in financial services, health care, electronic commerce, telecommunication, government, etc. With the rapid evolution of information technology, people are becoming even more and more electronically connected. As a result, the ability to achieve highly accurate automatic personal identification is becoming more critical. A wide variety of systems require reliable personal authentication schemes to either confirm or determine the identity of individuals requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed by a legitimate user, and not anyone else. Examples of these systems include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust authentication schemes, these systems are vulnerable to the wiles of an impostor. Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to systems. The major advantages of this traditional personal identification are that

(i) They are very simple

(ii) They can be easily integrated into different systems with a low cost.

However these approaches are not based on any inherent attributes of an individual to make a personal identification thus having number of disadvantages like tokens may be lost, stolen, forgotten, or misplaced; PIN may be forgotten or guessed by impostors. Security can be easily breached in these systems when a password is divulged to an unauthorized user or a card is stolen by an impostor; further, simple passwords are easy to guess (by an impostor) and difficult passwords may be hard to recall (by a legitimate user).Therefore they are unable to satisfy the security requirements of our electronically interconnected information society. The emergence of biometrics has addressed the problems that plague traditional verification.

Biometrics: In the world of computer security, biometrics refers to authentication techniques that rely on measurable physiological and individual characteristics that can be automatically verified. In other words, we all have unique personal attributes that can be used for distinctive identification purposes, including a fingerprint, the pattern of a retina, and voice characteristics. Strong or two-factor authentication—identifying oneself by two of the three methods of something you know (for example, a password), have (for example, a swipe card), or is (for example, a fingerprint)—is becoming more of a genuine standard in secure computing environments. Some personal computers today can include a fingerprint scanner where you place your index finger to provide authentication. The computer analyzes your fingerprint to determine who you are and, based on your identity followed by a pass code or pass phrase, allows you different levels of access. Access levels can include the ability to open sensitive files, to use credit card information to make electronic purchases, and so on.

Biometrics Authentication Techniques: A biometric authentication is essentially a pattern-recognition that makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. An important issue is designing a practical approach to determine how an individual is identified. An authentication can be divided into two modules:
a) Enrollment module
b) Identification or Verification module

How Biometric Technologies work: The enrollment module is responsible for enrolling individuals into the biometric system. During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a raw digital representation of the characteristic. In order to facilitate matching, the raw digital representation is usually further processed by feature extractor to generate a compact but expensive representation, called a template. Depending on the application, the template may be stored in the central database. Depending on the application, biometrics can be used in one of two modes: verification or identification. Verification—also called authentication—is used to verify a person's identity—that is, to authenticate that individuals are who they say they are. Identification is used to establish a person's identity—that is, to determine who a person is. Although biometric technologies measure different characteristics in substantially different ways, all biometric systems start with an enrollment stage followed by a matching stage that can use either verification or identification.

1. **Enrollment:** In enrollment, a biometric system is trained to identify a specific person. The person first provides an identifier, such as an identity card. The biometric is linked to the identity specified on the identification document. He or she then presents the biometric (e.g., fingertips, hand, or iris) to an acquisition device. The distinctive features are located and one or more samples are extracted, encoded, and stored as a reference template for future comparisons. Depending on the technology, the biometric sample may be collected as an image, a recording, or a record of related dynamic measurements. How biometric systems extract features and encode and store

information in the template is based on the system vendor's proprietary algorithms. Template size varies depending on the vendor and the technology. Templates can be stored remotely in a central database or within a biometric reader device itself; their small size also allows for storage on smart cards or tokens.

Minute changes in positioning, distance, pressure, environment, and other factors influence the generation of a template. Consequently, each time an individual's biometric data are captured, the new template is likely to be unique. Depending on the biometric system, a person may need to present biometric data several times in order to enroll. Either the reference template may then represent an amalgam of the captured data or several enrollment templates may be stored. The quality of the template or templates is critical in the overall success of the biometric application. Because biometric features can change over time, people may have to reenroll to update their reference template. Some technologies can update the reference template during matching operations. The enrollment process also depends on the quality of the identifier the enrollee presents. The reference template is linked to the identity specified on the identification document. If the identification document does not specify the individual's true identity, the reference template will be linked to a false identity.

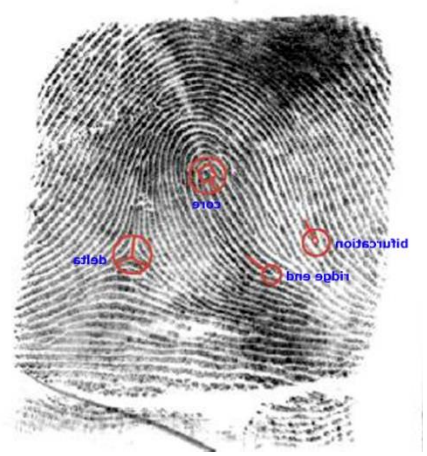
2. **Verification:** In verification systems, the step after enrollment is to verify that a person is who he or she claims to be (i.e., the person who enrolled). After the individual provides an identifier, the biometric is presented, which the biometric system captures, generating a trial template that is based on the vendor's algorithm. The system then compares the trial biometric template with this person's reference template, which was stored in the system during enrollment, to determine whether the individual's trial and stored templates match. Verification is often referred to as 1:1 (one-to-one) matching. Verification systems can contain databases ranging from dozens to millions of enrolled templates but are always predicated on matching an individual's presented biometric against his or her reference template. Nearly all verification systems can render a match–no-match decision in less than a second.

   One of the most common applications of verification is a system that requires employees to authenticate their claimed identities before granting them access to secure buildings or to computers
3. **Identification:** In identification systems, the step after enrollment is to identify who the person is. Unlike verification systems, no identifier is provided. To find a match, instead of locating and comparing the person's reference template against his or her presented biometric, the trial template is compared against the stored reference templates of all individuals enrolled in the system.

Identification systems are referred to as 1: M (one-to-M, or one-to-many) matching because an individual's biometric is compared against multiple biometric templates in the system's database. There are two types of identification systems: positive and negative. Positive identification systems are designed to ensure that an individual's biometric is enrolled in the database. The anticipated result of a search is a match. A typical positive identification system controls access to a secure building or secure computer by checking anyone who seeks access against a database of enrolled employees. The goal is to determine whether a person seeking access can be identified as having been enrolled in the system. Negative identification systems are designed to ensure that a person's biometric information is not present in a database. The anticipated result of a search is a no match. Comparing a person's biometric information against a database of all who are registered in a public benefits program, for example, can ensure that this person is not "double dipping" by using fraudulent documentation to register under multiple identities. Another type of negative identification system is a watch list system. Such systems are designed to identify people on the watch list and alert authorities for appropriate action. For all other people, the system is to check that they are not on the watch list and allow them normal passage. The people whose biometrics is in the database in these systems may not have provided them voluntarily. For instance, for a surveillance system, the biometric may be faces captured from mug shots provided by a law enforcement agency.

Matches based on threshold settings: No match is ever perfect in either verification or identification system, because every time a biometric is captured, the template is likely to be unique. Therefore, biometric systems can be configured to make a match or no-match decision, based on a predefined number, referred to as a threshold, which establishes the acceptable degree of similarity between the trial template and the enrolled reference template. After the comparison, a score representing the degree of similarity is generated, and this score is compared to the threshold to make a match or no-match decision. Depending on the setting of the threshold in identification systems, sometimes several reference templates can be considered matches to the trial template, with the better scores corresponding to better matches.

Fingerprints as a Biometric: Among all biometric traits, fingerprints have one of the highest levels of reliability and have been extensively used by forensic experts in criminal investigations. A fingerprint refers to the flow of ridge patterns in the tip of the finger. The ridge flow exhibits anomalies in local regions of the fingertip, and it is the position and orientation of these anomalies that are used to represent and match fingerprints.



Although not scientifically established, fingerprints are believed to be unique across individuals, and across fingers of the same individual. Even identical twins having similar DNA, are believed to have different fingerprints. Traditionally, fingerprint patterns have been extracted by creating an inked impression of the fingertip on paper.

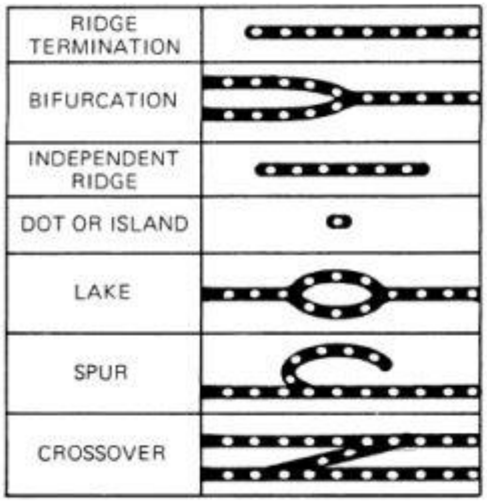
The electronic era has ushered in a range of compact sensors that provide digital images of these patterns. These sensors can be easily incorporated into existing computer peripherals like the mouse or the keyboard (figure), thereby making this mode of identification a very attractive proposition. This has led to the increased use of automatic fingerprint-based authentication systems in both civilian and law enforcement applications.

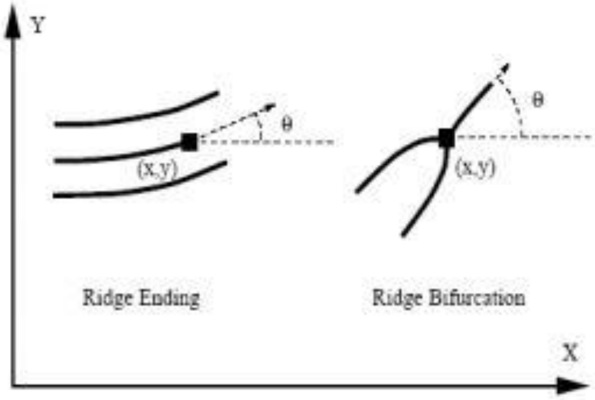
1. **Fingerprint Representation:** The uniqueness of a fingerprint is determined by the topographic relief of its ridge structure and the presence of certain ridge anomalies termed as minutiae points.

   Typically, the global configuration defined by the ridge structure is used to determine the class of the fingerprint, while the distribution of minutiae points is used to match and establish the similarity between two fingerprints.

   Automatic fingerprint identification systems, that match a query print against a large database of prints (which can consist of millions of prints), rely on the pattern of ridges in the query image to narrow their search in the database (fingerprint indexing), and on the minutiae points to determine an exact match (fingerprint matching). The ridge flow pattern itself is rarely used for matching fingerprints.

2. **Minutiae:** Minutiae, in fingerprinting terms, are the points of interest in a fingerprint, such as bifurcations (a ridge splitting into two) and ridge endings. Examples are:
   a) ridge endings - a ridge that ends abruptly
   b) ridge bifurcation - a single ridge that divides into two ridges
   c) short ridges, island or independent ridge - a ridge that commences, travels a short distance and then ends





   d) ridge enclosures - a single ridge that bifurcates and reunites shortly afterward to continue as a single ridge
   e) spur - a bifurcation with a short ridge branching off a longer ridge
   f) crossover or bridge - a short ridge that runs between two parallel ridges
   Minutiae also refer to any small or otherwise incidental details. But the focus when matching is only on the 2 main minutiae; ridge ending and ridge bifurcation.

PROBLEM DEFINITION

To propose a simple and effective approach for Biometric fingerprint image enhancement and minutiae extraction based on the frequency and orientation of the local ridges and thereby extracting correct minutiae points.

Automatic and reliable extraction of minutiae from fingerprint images is a critical step in fingerprint matching. The quality of input fingerprint images plays an important role in the performance of automatic identification and verification algorithms.

In this project, a fast fingerprint enhancement and minutiae extraction algorithm which improves the clarity of the ridge and valley structures of the input fingerprint images based on the frequency and orientation of the local ridges and thereby extracting correct minutiae is presented.

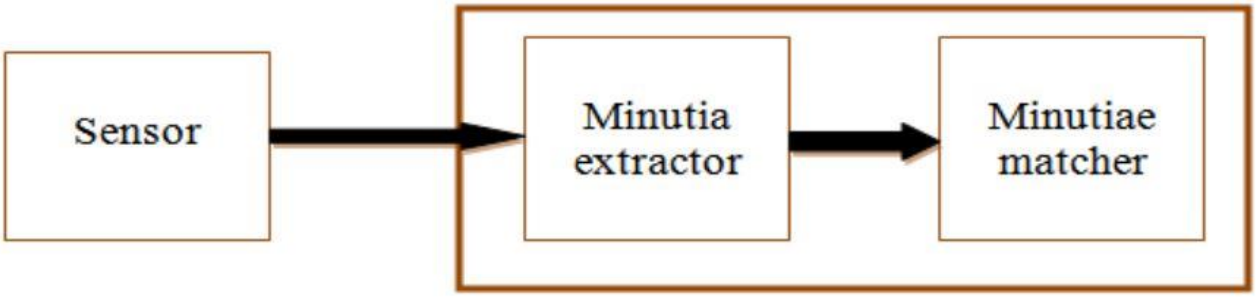
Fingerprint based identification has been one of the most successful biometric techniques used for personal identification. Each individual has unique fingerprints. A fingerprint is the pattern of ridges and valleys on the fingertip. A fingerprint is thus defined by the uniqueness of the local ridge characteristics and their relationships. Minutiae points are these local ridge characteristics that occur either at a ridge ending or a ridge bifurcation. A ridge ending is defined as the point where the ridge ends abruptly and the ridge bifurcation is the point where the ridge splits into two or more branches. Automatic minutiae detection becomes a difficult task in low quality fingerprint images where noise and contrast deficiency result in pixel configurations similar to that of minutiae. This is an important aspect that has been taken into consideration in this presentation for extraction of the minutiae with a minimum error in a particular location. A complete minutiae extraction scheme for automatic fingerprint recognition systems is presented. The proposed method uses improving alternatives for the image enhancement process, leading consequently to an increase of the reliability in the minutiae extraction task.

About the project: Fingerprint based identification has been one of the most successful biometric techniques used for personal identification. Each individual has unique fingerprints. A fingerprint is the pattern of ridges and valleys on the fingertip. A fingerprint is thus defined by the uniqueness of the local ridge characteristics and their relationships. Minutiae points are these local ridge characteristics that occur either at a ridge ending or a ridge bifurcation.

A ridge ending is defined as the point where the ridge ends abruptly and the ridge bifurcation is the point where the ridge splits into two or more branches. Automatic minutiae detection becomes a difficult task in low quality fingerprint images where noise and contrast deficiency result in pixel configurations similar to that of minutiae. This is an important aspect that has been taken into consideration in this presentation for extraction of the minutiae with a minimum error in a particular location.

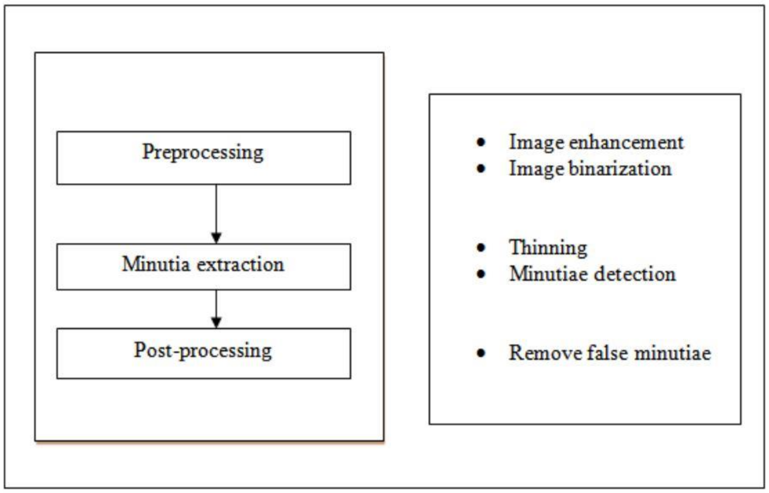
SYSTEM DESIGN

System Level Design: A fingerprint recognition system constitutes of fingerprint acquiring device, minutia extractor and minutia matcher.

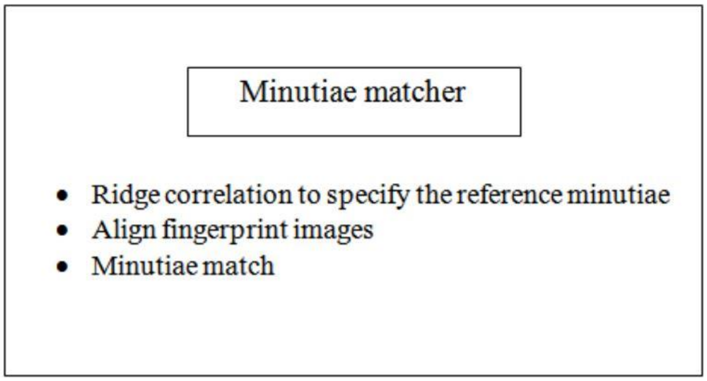


For fingerprint acquisition, optical or semi-conduct sensors are widely used. They have high efficiency and acceptable accuracy except for some cases that the user's finger is too dirty or dry. However, the testing database for this project consists of fingerprints taken from online database. FVC2002 Database.
(site: http://bias.csr.unibo.it/fvc2002/)

Algorithm Level design: To implement a minutia extractor, a three-stage approach is widely used by researchers. They are preprocessing, minutia extraction and post-processing stage.



For the fingerprint image preprocessing stage, several image processing techniques are used to do image enhancement. And then the fingerprint image is binarized using the locally adaptive threshold method. The image segmentation task is fulfilled by a three-step approach: block direction estimation, segmentation by direction intensity and Region of Interest extraction by Morphological operations. For minutia extraction stage, iterative parallel thinning algorithm is used. The minutia marking is a relatively simple task. For the post-processing stage, a more rigorous algorithm is developed to remove false minutia. The minutia matcher chooses any two minutiae as a reference minutia pair and then matches their associated ridges first. If the ridges match well, the two fingerprint images are aligned and matching is conducted for all the remaining minutiae.



Minutiae matcher

- Ridge correlation to specify the reference minutiae
- Align fingerprint images
- Minutiae match

FINGERPRINT IMAGE – PREPROCESSING

Image Enhancement: Fingerprint Image enhancement is used to make the image clearer for easy further operations. Since the fingerprint images acquired from scanner or any other media are not assured with perfect quality, those enhancement methods, for increasing the contrast between ridges and valleys and for connecting the false broken points of ridges due to insufficient amount of ink, are very useful for keep a higher accuracy to fingerprint recognition.

Several steps are followed in enhancing the image to finally getting a thinned image of the fingerprint

Fourier Transform: We divide the image into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to,

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times \exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\}$$

In order to enhance a specific block by its dominant frequencies, we multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original
FFT = abs(F(u,v)) = |F(u,v)|
We get the enhanced block according to

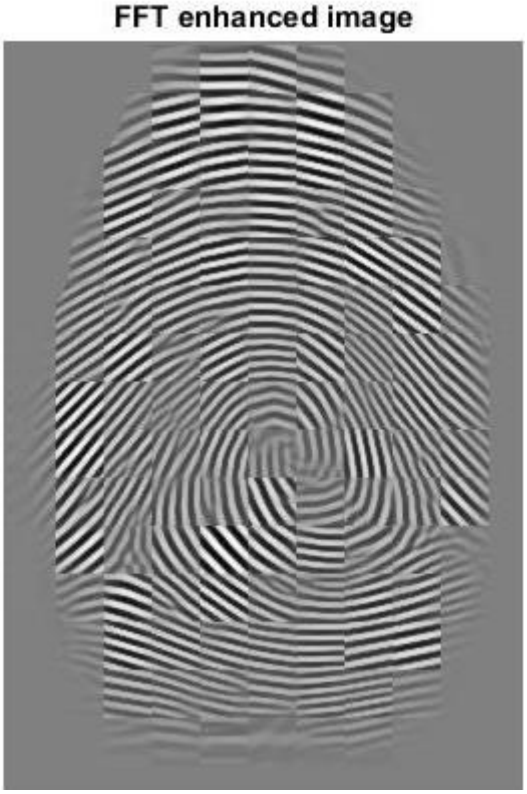
$$g(x,y) = F^{-1}\left\{F(u,v) \times \left|F(u,v)\right|^{K}\right\}$$

where $F^{-1}(F(u,v))$ is done by

$$f(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v) \times \exp\left\{ j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N} \right) \right\}$$

The enhanced image after FFT has the improvements to connect some falsely broken points on ridges and to remove some false connections between ridges.

After enhancing the image using we get the following image,



Ridge Segmentation: This is used to normalize the fingerprint image and segment ridge regions.

The function used here identifies ridge regions of a fingerprint image and returns a mask identifying this region. It also normalizes the intensity values of the image so that the ridge regions have zero mean, unit standard deviation.

This function breaks the image up into blocks of size blksze x blksze and evaluates the standard deviation in each region. If the standard deviation is above the threshold it is deemed part of the fingerprint. Image is normalized to have zero mean, unit standard deviation prior to performing this process so that the threshold you specify is relative to a unit standard deviation.

Normalized image

Ridge Orientation: This is used to estimate the local orientation of ridges in a fingerprint.
First, Image gradients are calculated using filters, then local ridge orientation at each point is estimated by finding the principal axis of variation in the image gradients. After this, covariance data for the image gradients is smoothened to perform a weighted summation of data. Reliability of the orientation data is calculated. We calculate the area moment of inertia about the orientation axis found (this will be the minimum inertia) and an axis perpendicular (which will be the maximum inertia). The reliability measure is given by 1.0-min_inertia/max_inertia. The reasoning being that if the ratio of the minimum to maximum inertia is close to one we have little orientation information.
Finally reliability is masked to exclude regions where the denominator in the orientation calculation above was small. Here it's set to the value to 0.001
Ridge Frequency: This is used to calculate the ridge frequency image.
Function to estimate the fingerprint ridge frequency across a fingerprint image. This is done by considering blocks of the image and determining a ridge count within each block.
Ridge Filter: This is used to enhance the fingerprint image using oriented filters. After this filter function is applied on the image, we get a binary image, which looks as follows

Binary Image

Masking or Extracting Region of Interest (ROI): In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges is first discarded since it only holds background information and probably noise. Then the bound of the remaining effective area is sketched out since the minutiae in the bound region are confusing with those false minutiae that are generated when the ridges are out of the sensor.

To extract the ROI, a two-step method is used. The first step is block direction estimation and direction variety check, while the second is done using some Morphological methods.

1. Block direction estimation: Estimate the block direction for each block of the fingerprint image with WxW in size (W is 16 pixels by default). The algorithm does the following:

   I. Calculates the gradient values along x-direction (g_x) and y-direction (g_y) for each pixel of the block. Two Sobel filters are used to fulfill the task.

   II. For each block, it uses the following formula to get the Least Square approximation of the block direction.

   $\tan 2ß = 2 \sum\sum (g_x{}^{*}g_y) / \sum\sum (g_x{}^2 - g_y{}^2)$ for all the pixels in each block.

   The formula is easy to understand by regarding gradient values along x-direction and y-direction as cosine value and sine value. So the tangent value of the block direction is estimated nearly the same as the way illustrated by the following formula.

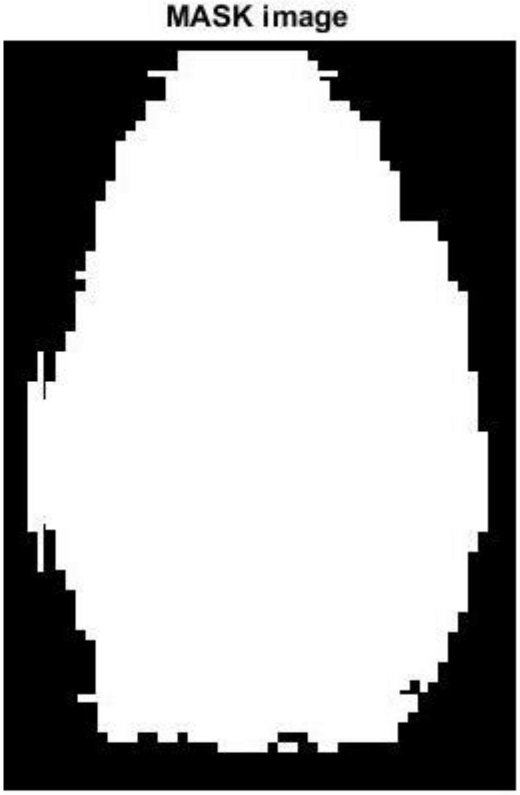
$\tan 2\O = 2\sin \O \cos \O /(\cos^2 \O - \sin^2 \O)$

After finishing with the estimation of each block direction, those blocks without significant information (ridges) are discarded based on the following formulas:

$E = \{2 \sum\sum (g_x{}^* g_y) + \sum\sum (g_x^2 - g_y^2)\} / W^*W^* \sum\sum (g_x^2 + g_y^2)$

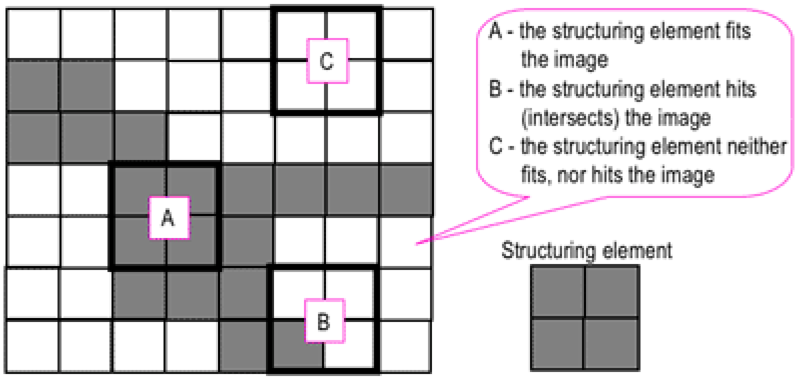
For each block, if its certainty level (E) is below a threshold, then the block is regarded as a background block.

After this we see mask image which follows,



2. Morphological image processing is a collection of non-linear operations related to the shape or morphology of features in an image. According to Wikipedia, morphological operations rely only on the relative ordering of pixel values, not on their numerical values, and therefore are especially suited to the processing of binary images. Morphological operations can also be applied to greyscale images such that their light transfer functions are unknown and therefore their absolute pixel values are of no or minor interest.

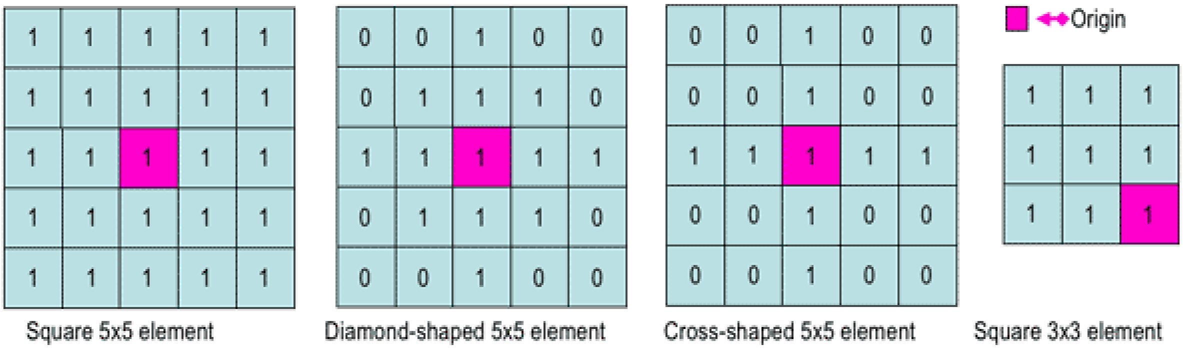
Morphological techniques probe an image with a small shape or template called a structuring element. The structuring element is positioned at all possible locations in the image and it is compared with the corresponding neighborhood of pixels. Some operations test whether the element "fits" within the neighborhood, while others test whether it "hits" or intersects the neighborhood:


C
A
B
A - the structuring element fits the image
B - the structuring element hits (intersects) the image
C - the structuring element neither fits, nor hits the image
Structuring element

Probing of an image with a structuring element (white and grey pixels have zero and non-zero values, respectively).

A morphological operation on a binary image creates a new binary image in which the pixel has a non-zero value only if the test is successful at that location in the input image.
The structuring element is a small binary image, i.e. a small matrix of pixels, each with a value of zero or one:

- The matrix dimensions specify the size of the structuring element.
- The pattern of ones and zeros specifies the shape of the structuring element.
- An origin of the structuring element is usually one of its pixels, although generally the origin can be outside the structuring element.



Square 5x5 element

1	1	1	1	1
1	1	1	1	1
1	1	1	1	1
1	1	1	1	1
1	1	1	1	1

Diamond-shaped 5x5 element

0	0	1	0	0
0	1	1	1	0
1	1	1	1	1
0	1	1	1	0
0	0	1	0	0

Cross-shaped 5x5 element

0	0	1	0	0
0	0	1	0	0
1	1	1	1	1
0	0	1	0	0
0	0	1	0	0

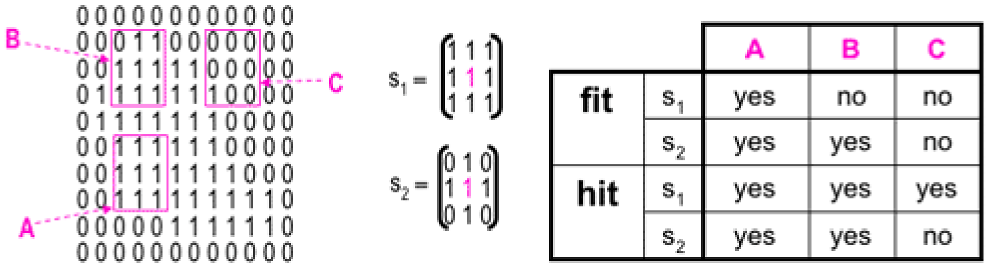
Square 3x3 element

1	1	1
1	1	1
1	1	1

Examples of simple structuring elements.

A common practice is to have odd dimensions of the structuring matrix and the origin defined as the center of the matrix. Structuring elements play in morphological image processing the same role as convolution kernels in linear image filtering.

When a structuring element is placed in a binary image, each of its pixels is associated with the corresponding pixel of the neighborhood under the structuring element. The structuring element is said to fit the image if, for each of its pixels set to 1, the corresponding image pixel is also 1. Similarly, a structuring element is said to hit, or intersect, an image if, at least for one of its pixels set to 1 the corresponding image pixel is also 1.



```
0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 1 1 0 0 0 0 0 0 0
0 0 1 1 1 1 1 0 0 0 0 0
0 1 1 1 1 1 1 1 0 0 0 0
0 1 1 1 1 1 1 1 0 0 0 0
0 0 1 1 1 1 1 1 0 0 0 0
0 0 1 1 1 1 1 1 1 0 0 0
0 0 1 1 1 1 1 1 1 1 1 0
0 0 0 0 0 1 1 1 1 1 1 0
0 0 0 0 0 0 0 0 0 0 0 0
```

$$s_1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$s_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

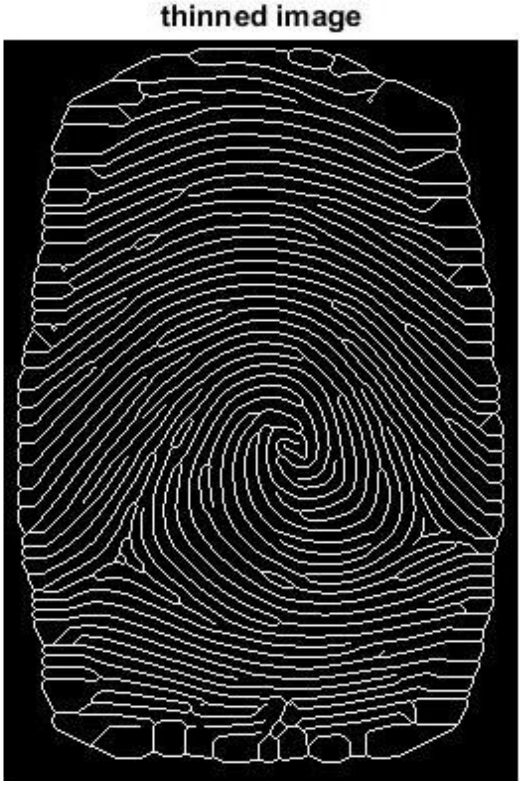
		A	B	C
fit	s_1	yes	no	no
	s_2	yes	yes	no
hit	s_1	yes	yes	yes
	s_2	yes	yes	no

Fitting and hitting of a binary image with structuring elements s1 and s2.

Zero-valued pixels of the structuring element are ignored, i.e. indicate points where the corresponding image value is irrelevant.

Here, the image is undergone erosion to have a thinned image of fingerprint such that all the ridges have a width of 1 pixel Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide.

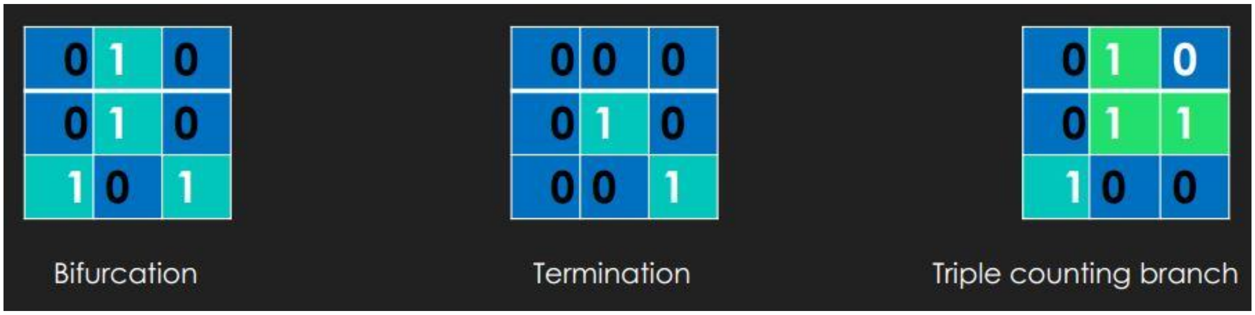
After this morphological operation we get an image as follows;



MINUTIAE EXTRACTION:

Minutiae Marking: After the fingerprint ridge thinning, marking minutia points is relatively easy. The concept of Crossing Number (CN) is widely used for extracting the
minutiae.

In general, for each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending, i.e., for a pixel P, if Cn(P) = = 1 it's a ridge end and if Cn(P) = = 3 it's a ridge bifurcation point.



0	1	0
0	1	0
1	0	1

Bifurcation

0	0	0
0	1	0
0	0	1

Termination

0	1	0
0	1	1
1	0	0

Triple counting branch

Figure 3 illustrates a special case that a genuine branch is triple counted. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3x3 window, so the two pixels will be marked as branches too, but actually only one branch is located in the small region. So a check routine requiring that none of the neighbors of a branch are branches is added.

Also the average inter-ridge width D is estimated at this stage. The average inter-ridge width refers to the average distance between two neighboring ridges. The way to approximate the D value is simple. Scan a row of the thinned ridge image and sum up all pixels in the row whose values are one. Then divide the row length by the above summation to get an inter-ridge width. For more accuracy, such kind of row scan is performed upon several other rows and column scans are also conducted, finally all the inter-ridge widths are averaged to get the D. Together with the minutia marking, all thinned ridges in the fingerprint image are labeled with a unique ID for further operation.

MINUTIAE POST-PROCESSING:

False Minutia Removal: The preprocessing stage does not usually fix the fingerprint image in total. For example, false ridge breaks due to insufficient amount of ink and ridge cross connections due to over inking are not totally eliminated. Actually all the earlier stages themselves occasionally introduce some artifacts which later lead to spurious minutia. These false minutiae will significantly affect the accuracy of matching if they are simply regarded as genuine minutiae. So some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective.

Seven types of false minutia are specified in following diagrams:

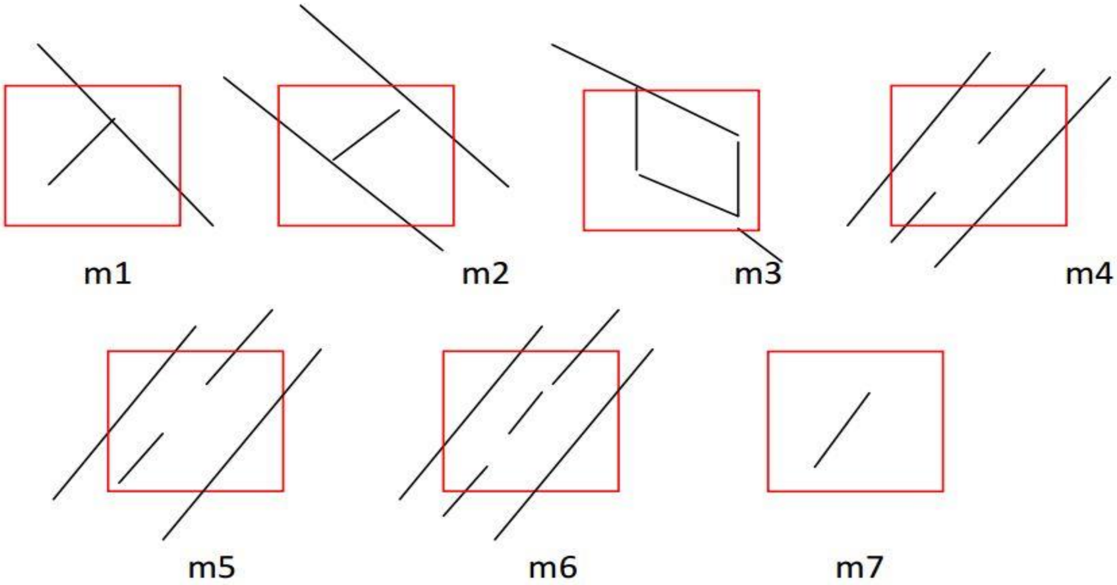


Figure: False Minutia Structures. m1 is a spike piercing into a valley. In the m2 case a spike falsely connects two ridges. m3 has two near bifurcations located in the same ridge. The two ridge broken points in the m4 case have nearly the same orientation and a short distance. m5 is alike the m4 case with the exception that one part of the broken ridge is so short that another termination is generated. m6 extends the m4 case but with the extra property that a third ridge is found in the middle of the two parts of the broken ridge. m7 has only one short ridge found in the threshold window.

The procedure for the removal of false minutia consists of the following steps:

1. If the distance between one bifurcation and one termination is less than D and the two minutiae are in the same ridge (m1 case). Remove both of them. Where D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.
2. If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations. (m2, m3 cases).
3. If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that no any other termination is located between the two terminations. Then the two terminations are regarded as false minutiae derived from a broken ridge and are removed. (Cases m4, m5 & m6).
4. If two terminations are located in a short ridge with length less than D, remove the two terminations (m7).

This procedure in removing false minutia has two advantages. One is that the ridge ID is used to distinguish minutia and the seven types of false minutia are strictly defined. The second advantage is that the order of removal procedures is well considered to reduce the computation complexity because it utilizes the relations among the false minutia types. For example, the procedure 3 solves the m4, m5 and m6 cases in a single check routine. And after procedure 3, the number of false minutia satisfying the m7 case is significantly reduced.

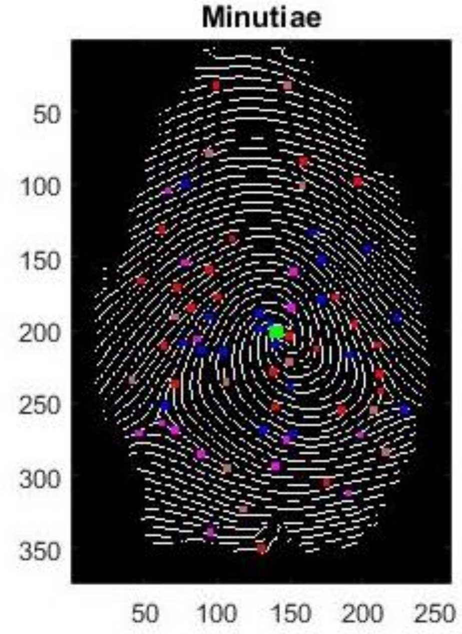


Image after removing false minutiae

MINUTIAE MATCH:

Given two set of minutia of two fingerprint images, the minutia match algorithm determines whether the two minutia sets are from the same finger or not.

An alignment-based match algorithm is used in my project. It includes two consecutive stages: one is alignment stage and the second is match stage.

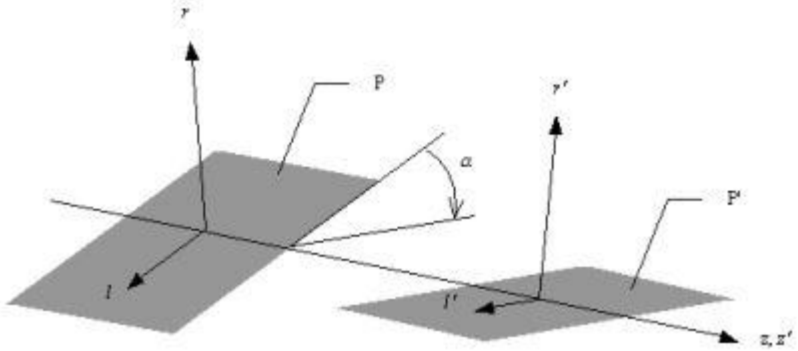
1. Alignment stage: Given two fingerprint images to be matched, choose any one minutia from each image; calculate the similarity of the two ridges associated with the two referenced minutia points. If the similarity is larger than a threshold, transform each set of minutia to a new coordination system whose origin is at the reference point and whose x axis is coincident with the direction of the referenced point.

2. Match stage: After we get two set of transformed minutia points, we use the matching algorithm to count the matched minutia pairs by assuming two minutia having nearly the same position and direction are identical.

Both the images are transformed such that they have same reference coordinates using the following equation:

$$\begin{pmatrix} xi\_new \\ yi\_new \\ \theta i\_new \end{pmatrix} = TM * \begin{bmatrix} (xi - x) \\ (yi - y) \\ (\theta i - \theta) \end{bmatrix} \quad \text{Where,} \quad TM = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The following diagram illustrates the rotation of the coordinate system according to the reference minutia's orientation:



This method uses the rotation angle calculated earlier by tracing a short ridge start from the minutia with length D. And since the rotation angle is already calculated and saved along with the coordinates of each minutiae, then this saves some processing time. The following step is to transform each minutia according to its own reference minutia and then match them in a unified x-y coordinate.

The matching algorithm for the aligned minutia patterns needs to be adaptive since the strict match requires that all parameters (x, y, Ø) are the same for two identical minutiae which is impossible to get when using biometric-based matching.

After the coordinate transformation, taking one image as the reference, the other images is rotated such that it's almost aligned with reference image to calculate similarity measure in the further steps. A bounding box is placed around each template minutia. If the minutia to be matched is within the rectangle box and the direction difference between them is less than a threshold, then, the two minutiae are regarded as a matched minutia pair. Here, we put thresholds on Euclidean distance from the rectangular box and angle (direction of minutia) and they are 15 and 14 for distance and angle respectively. Each time a minutia pair is found by satisfying this criteria, we increase the score by 1. And this process is continued as long as the whole image is covered and the final score value is noted.

Now, using this score value, similarity measure is calculated. The formula used to find the similarity measure is;

$$SM = \sqrt[2]{\frac{n^2}{a * b}}$$

Where, a and b are the size of the transformed image after minutia extraction and n is the score value.

From the graphs of False matching rate and False non-matching rate, it's found that the threshold for similarity measure is 0.48, which means two fingerprints are said to be matching if the similarity measure is more than 0.48

And thus, the matching process of two fingerprints is done and we get the results whether the fingerprints are Match or not.

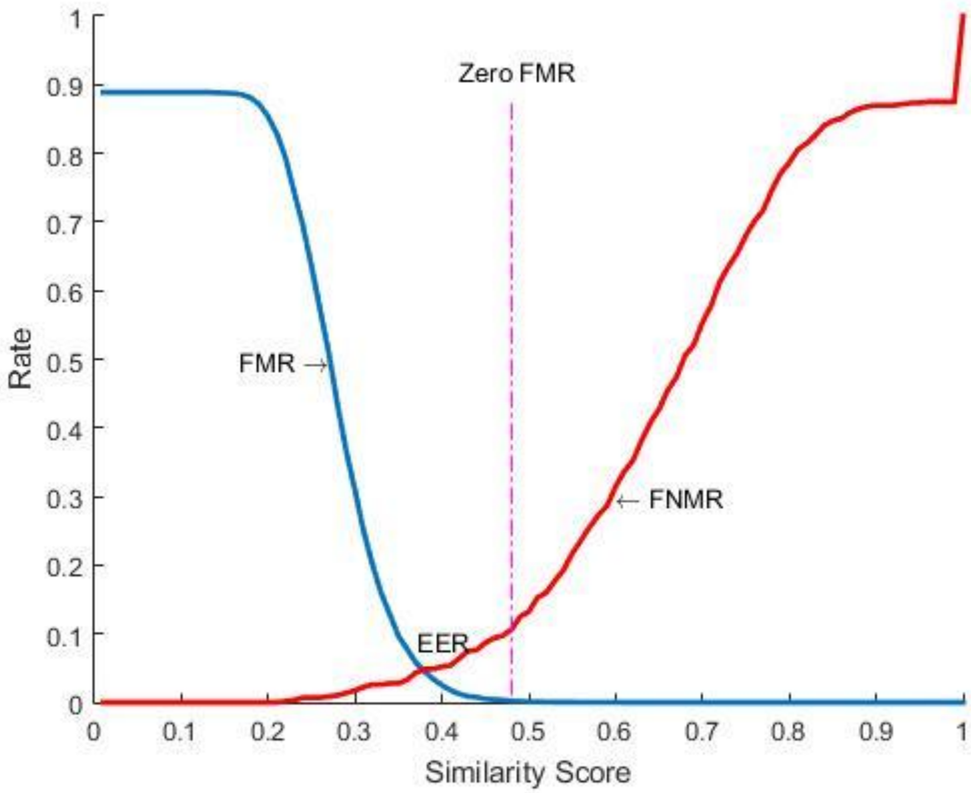
Here, two cases of matching are considered.

1. One to one matching - In this case we want to find if the two taken fingerprints are of the same person or not. Both the fingerprints are fed into the system and results are derived to know if it's a match. This is useful in applications such as crime detection, where we want to compare between available samples of fingerprints.
2. One to many matching – In this case, an arbitrary fingerprint is taken and fed to the system. The program runs to find out if there are any matching fingerprints present in the database. This is useful in applications such as attendance register in companies, authenticating someone for restricted access etc.

SYSTEM EVALUATION AND CONCLUSION:

Observations:

1. When altering in such an important step such as the image enhancement part, the performance quality of the system drops rapidly as the noise in the image is increased. Because when working with a biometric identification system, obtaining clear and noise free images is a really hard thing, so this step is usually needed.
2. For the binarization step, as explained earlier, using global thresholding may introduce a few problems and may lead to the elimination of significant details by mistake. Setting the threshold at 120 (although it's almost the average value for a gray-scale image) affected the system performance a lot and led to false non-match results, while setting a fixed threshold as low as 80 gave better results. Still, it remains better to use the adaptive threshold method because, although it consumes more processing time, it still guarantees the quality of the results.
3. The following graph shows the variations between similarity score and the false matching and false non-matching rates. We find zero FMR at a similarity score of 0.48.



CONCLUSION:

1. The proposed algorithm is a simple approach towards matching two fingerprints by counting number minutiae pair with help of similarity measure.
2. The reliability of any automatic fingerprint system strongly relies on the precision obtained in the minutia extraction process.
3. Poor image quality damages the correct location of minutia.
4. There is a scope of further improvement in terms of efficiency and accuracy which can be achieved by improving the hardware to capture the image or by improving the image enhancement techniques. So that the input image to the thinning stage could be made better, this could improve the future stages and the final outcome.

REFERENCES:

1. Fingerprint matching – Anil K. Jain, Jianjiang Feng, Karthik Nandakumar
2. Fingerprint matching using orientation based minutia descriptor by Marius Tico, Pauli Kuosmanen
3. A minutia based partial fingerprint recognition system by Tsai-Yang Jea, Venu Govindaraju
4. Combining multiple matchers for a high security fingerprint verification system by Anil K. Jain, Salil Prabhakar, Shaoyun Chen
5. A hybrid fingerprint matcher by Arun Ross, Anil Jain, James Reisman
6. A minutiae-based matching algorithms in fingerprint recognition systems – Journal medical informatics & technologies, Vol 13/2009, ISSN 1642-6037
7. Fingerprint recognition using minutia score matching by Ravi J., K. B. Raja, Venugopal K. R
8. Journal of Electronic Imaging/Mehmet Sezgin and Bulent Sankur; Survey over image thresholding techniques and quantitative performance evaluation/Jan.2004