BIOMETRIC VERIFICATION SYSTEM USING FINGERPRINT IMAGE AT LEVEL 2

Enrollment no. - 101449

Name of Student - Shivani Garg

Name of Supervisor - Mr. Amit Kumar Singh

Submitted in partial fulfillment of the degree of bachelor of technology

DEPARTMENT OF COMPUTER SCIENC AND ENGINEERING/INFORMATION

TECHNOLOGY

JAYPEE UNIVERSITY OF INFORMATION AND TECHNOLOGY

WAKNAGHAT

Table of Contents

Chapter 1: Introduction

Chapter 2: Background and Literature Review

Chapter 3: Proposed Work

Chapter 4: Experimental Results

<u>CERTIFICATE</u>

This is to certify that the work titled "***BIOMETRIC VERIFICATION SYSTEM USING FINGERPRINT IMAGE AT LEVEL 2***" submitted by "***SHIVANI GARG***" in partial fulfillment for the award of degree of B. Tech of Jaypee University of Information Technology, Waknaghat has been carried out under my supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor ……………………..

Name of Supervisor Mr. Amit Kumar Singh

Designation

Date

ACKNOWLEDGEMENT

The project in this report is an outcome of continual work over and intellectual support from various sources. It is therefore almost impossible to express adequately the debts owed to many persons who have been instrumental in imparting this work, a successful status .It is however a matter of pleasure to express our gratitude and appreciation to those who have been contributing to bring about this project.

We take this opportunity to thank our esteemed mentor and supervisor Mr. Amit Kumar Singh, Department of Computer Science and Engineering/Information Technology, JUIT, for lending me stimulating suggestions, innovative quality guidance and creative thinking. His practicality, constructive criticism, constant encouragement and advice helped us in all stages of the project. His scientific views and scientific approach will always be the source of motivation for us. I am grateful to him for the support, he provided in doing things at our pace and for being patient with our mistakes.

Signature of the student ……………………..
Name of Student Shivani Garg
Date ……………………..

ABSTRACT

Human fingerprints are rich in details called minutiae, which can be used as identification marks for fingerprint verification. The goal of this project is to develop a complete system for fingerprint verification through extracting and matching minutiae. To achieve good minutiae extraction in fingerprints with varying quality, preprocessing in form of image enhancement and binarization is first applied on fingerprints before they are evaluated. Many methods have been combined to build a minutia extractor and a minutia matcher. Minutia-marking with false minutiae removal methods are used in the work. An alignment-based elastic matching algorithm has been developed for minutia matching. This algorithm is capable of finding the correspondences between input minutia pattern and the stored template minutia pattern without resorting to exhaustive search. Performance of the developed system is then evaluated on an online fingerprint database.

Shivani Garg	Mr. Amit Kumar Singh
Date:	Date:

CHAPTER 1: INTRODUCTION

1. Why Biometrics?

Biometrics is an advanced technology for superb security and authentication. The very term "biometric” it represent that "bio" means related to the biological study and "metric "means something, which is related to measurement. "Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. However, biometric identification has eventually a much broader relevance as computer interface becomes more natural. Knowing the person with whom you are conversing is an important part of human interaction and one expects computers of the future to have the same capabilities. A number of biometric traits have been developed and are used to authenticate the person's identity. The idea is to use the special characteristics of a person to identify him. By using special characteristics we mean the using the features such as face, iris, fingerprint, signature etc. The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods for various reasons such as: The person to be identified is required to be physically present at the time-of-identification. Identification based on biometric techniques obviates the need to remember a password or carry a token. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic".

1.2 Difference between Biometrics and Forensic

While both biometrics and forensics involve human recognition

i) Biometrics is typically applied using automated techniques to pre-event situation application, such as gaining access to sensitive information or to a secured facility whereas forensic applications typically occur after a crime has occurred and may not use fully automated methods.

ii) Biometric is the science and technology of verifying a person's identity whereas forensics is the science and technology of using and interpreting physical evidence for legal purposes.

iii)Biometric measures the physical characteristics that make each of us unique, like the fingerprints, an eye's retina or iris, a face, a hand, a voice - and uses those measurements to confirm personal identity whereas forensics are related to processing and interpreting image data, image enhancement, detection of characteristic landmarks.

iv) Passwords are difficult to remember and easy to steal. Keys, driver's licenses and passports can be lost or forged. The human body, on the other hand, can't be forgotten, stolen, forged or misplaced. Practical uses for such biometrics are wide spread and include maintaining the security for both physical space and cyberspace.

v) Biometric is used in the field of fingerprint analysis, impression analysis, smart cards, biometric identification etc. whereas Forensic is used in the field of corpse identification, criminal investigation, missing children etc.

1.3 Characteristics of Biometric System:

The selection of a particular biometric for use in a specific application involves a weighting of several factors. They are:

i) Universality**:**

It means that every person using a system should possess the trait.

ii) Distinctiveness**:**

It means that the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.

iii) Permanence**:**

It relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.

iv) Collectability**:**

It relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.

v) Performance**:**

It relates to the accuracy, speed, and robustness of technology used.

vi) Acceptability**:**

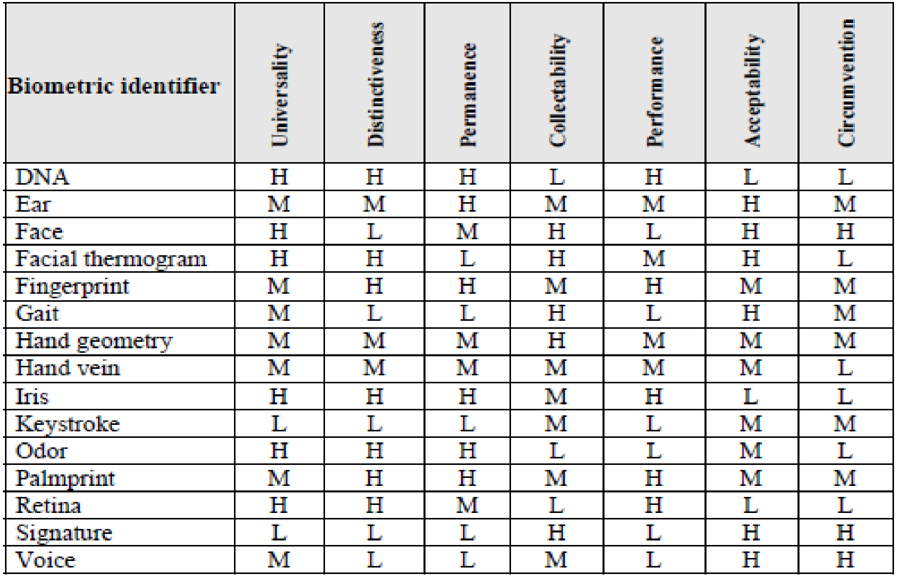
It relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.

vii) Circumvention:

It relates to the ease with which a trait might be imitated using an artifact or substitute.

Comparison of different biometric traits

TABLE 1: Comparison of different biometric traits



Biometric identifier	**Universality**	**Distinctiveness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Motivation

Reliable user authentication is becoming an increasingly important task in the Web enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer or network access. Many other applications in everyday life also require user authentication, such as banking, e-commerce, and physical access control to computer resources, and could benefit from enhanced security. The basic need of using biometric system is that biometric offers natural and reliable solution to the problem of identity determination by recognizing individual by using certain physiological traits such as fingerprint, face or some behavioral traits.

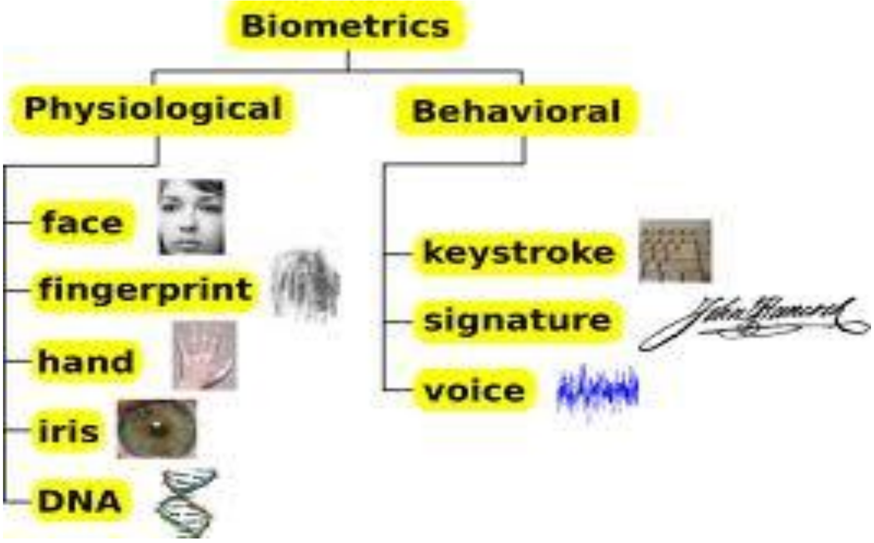


Figure 1: Biometrics Traits

1.4 What is A Fingerprint?

A fingerprint is the feature pattern of one finger (Figure 1.4.1). It is believed with strong evidences that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and forensic investigation for a long time.

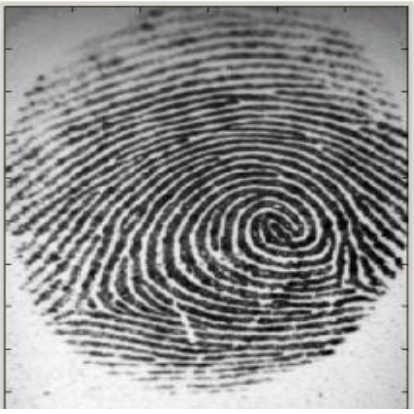


Figure1.4.1 A fingerprint image acquired by an Optical Sensor

A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width.

However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges (Figure 1.4.2). Among the variety of minutia types reported in literatures, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive.

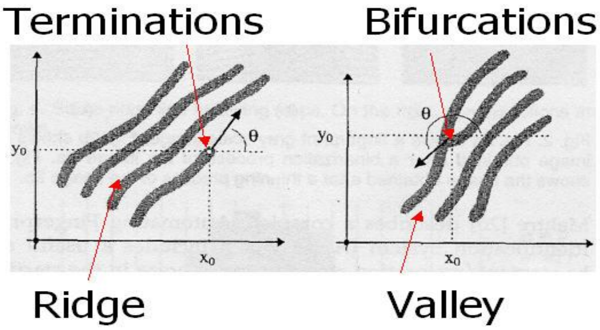


Figure 1.4.2 Minutia (Valley is also referred as Furrow, Termination is also called Ending, and Bifurcation is also called Branch)

1.5 What is Fingerprint Recognition?

The fingerprint recognition problem can be grouped into two sub-domains: one is fingerprint verification and the other is fingerprint identification (Figure 1.5.1). In addition, different from the manual approach for fingerprint recognition by experts, the fingerprint recognition here is referred as AFRS (Automatic Fingerprint Recognition System), which is program-based.

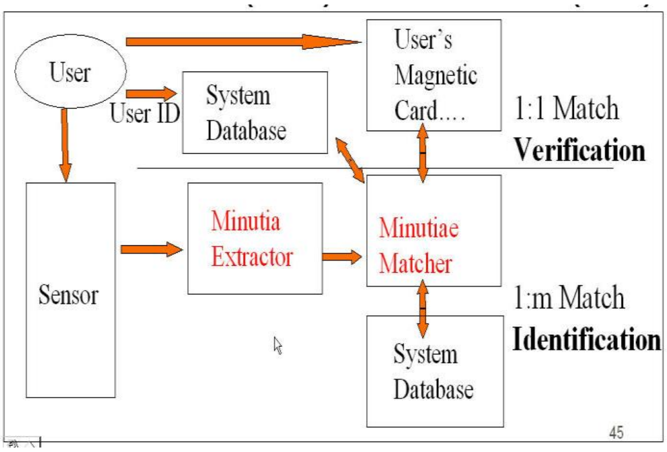


Figure 1.5.1 Verification vs. Identification

Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his ID number. The fingerprint verification system retrieves the fingerprint template according to the ID number and matches the template with the real-time acquired fingerprint from the user. Usually it is the underlying design principle of AFAS (Automatic Fingerprint Authentication System).

Fingerprint identification is to specify one person’s identity by his fingerprint(s). Without knowledge of the person’s identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database. It is especially useful for criminal investigation cases. And it is the design principle of AFIS (Automatic Fingerprint Identification System).

However, all fingerprint recognition problems, either verification or identification, are ultimately based on a well-defined representation of a fingerprint. As long as the representation of fingerprints remains the uniqueness and keeps simple, the fingerprint matching, either for the 1-to-1 verification case or 1-to-m identification case, is straightforward and easy.

1.5.1 Fingerprint verification Process

Fingerprint verification is the method where we compare a claimed fingerprint with an enroll fingerprint, where our aim is to match both the fingerprints. This method is mainly used to verify a person’s authenticity. For verification a person needs to his or her fingerprint in to the fingerprint verification system. Then this representation is saved in some compress format with the person’s identity and his or her name. Then it is applied to the fingerprint verification system so that the person’s identity can be easily verified. Fingerprint verification is also called, one-to-one matching.

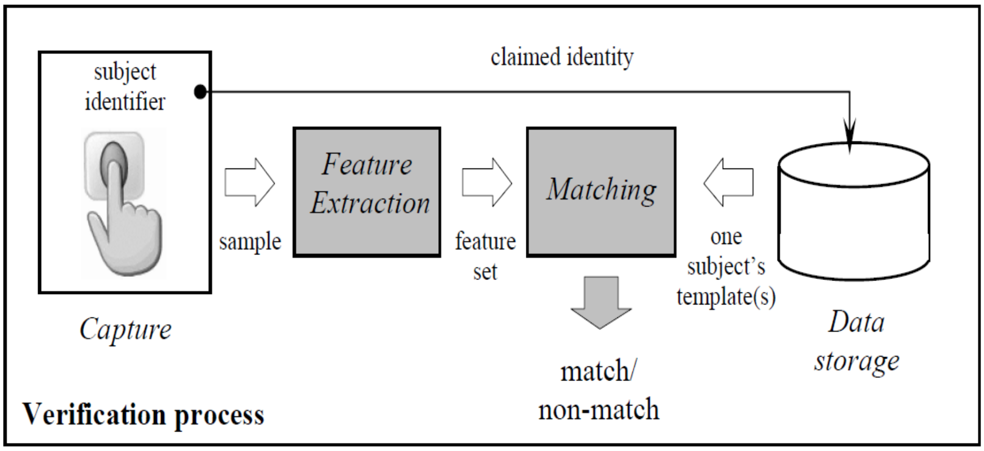


Figure 2: Fingerprint Verification System

In verification, the user claims an identity and the system verifies whether the claim is genuine, i.e., the system answers the question “Are you who you say you are?". In this scenario, the query is compared only to the template corresponding to the claimed identity. If the user's input and the template of the claimed identity have a high degree of similarity, then the claim is accepted as “genuine”. Otherwise, the claim is rejected and the user is considered an “impostor”. Formally, verification can be posed as the following two-category classification problem:

Given a claimed identity *I* and a query feature set *XQ*, we need to decide if (*I*, *XQ*) belong to “genuine” or “impostor” class. Let *XI* be the stored template corresponding to identity *I*. Typically, *XQ* is compared with *XI* and a *match score S*, which measures the similarity between *XQ* and *XI*, is computed. The decision rule is given by

$$(I, XQ) \in \begin{cases} \text{Genuine} & \text{if } S >= Th, \\ \text{Impostor} & \text{if } S < Th, \end{cases}$$

Where, Th is a pre-defined threshold. In this formulation, the match score *S* is assumed to measure the similarity between *XQ* and *XI*, i.e., a large score indicates a good match. It is also possible for the match score to be a dissimilarity or distance measure (i.e., a large score indicates a poor match) and in this case, the inequalities in the decision rule shown in the above equation should be reversed.

1.5.2 Fingerprint Identification Process

Fingerprint identification is mainly used to specify any person’s identity by his fingerprint. Identification has been used for criminal fingerprint matching. Here the system matches the fingerprint of unknown ownership against the other fingerprints present in the database to associate a crime with identity. This process is also called, one-to- many matching. Identification is traditionally used for solve crime and catch thieves.

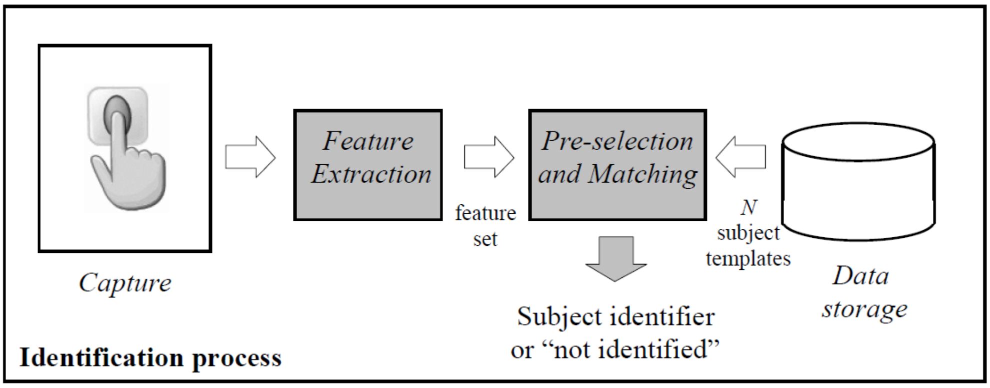


Figure 3: Fingerprint Identification System

Identification functionality can be classified into positive and negative identification. In positive identification, the user attempts to positively identify him to the system without explicitly claiming an identity. A positive identification system answers the question “Are you someone who is known to the system?" by determining the identity of the user from a known set of identities. In contrast, the user in a negative identification application is considered to be concealing his true identity from the system. Negative identification is also known as screening and the objective of such systems is to find out “Are you who you say you are not?". Screening is often used at airports to verify whether a passenger's identity matches with any person on a “watch-list". Screening can also be used to prevent the issue of multiple credential records (e.g., driver's license, passport) to the same person. Negative identification is also critical in applications such as welfare disbursement to prevent a person from claiming multiple benefits (i.e., double dipping) under different names. In both positive and negative identification, the user's biometric input is compared with the templates of all the persons enrolled in the database and the system outputs either the identity of the person whose template has the highest degree of similarity with the user's input or a decision indicating that the user presenting the input is not an enrolled user. Formally, the problem of identification can be stated as follows:

Given a query feature set XQ, we need to decide the identity I of the user, where I € {I1, *I2, IN, IN+1*}. Here, *I1, I2, IN* correspond to the identities of the N users enrolled in the system and *IN+1* indicates the case where no suitable identity can be determined for the given query. If *X*In is the stored template corresponding to identity *In* and *Sn* is the match (similarity) score between XQ and *X*In, for n = 1, 2. . . N, the decision rule for identification is,

$$XQ \in \begin{cases} In0 & \text{if } n0 = \arg\max_{n} Sn \text{ and } Sn0 >= Th \\ IN+1, & \text{otherwise,} \end{cases}$$

Where, Th is a predefined threshold.

Comparison between verification and identification system:

i) Verification is less expensive than identification.
ii) Verification is more accurate than identification.
iii) Verification requires less processing power than identification.
iv) Verification is faster than identification.
v) Identification system is more convenient than verification.

1.6 Applications

The area of application of biometrics has been increased and it is expected that in the near future we will use biometry many times in our daily activities such as getting in the car, opening the door of our house, accessing to our bank account, shopping by internet, mobile phone, laptops, etc. Depending on where the biometric is deployed, the application can be categorized in the following five main groups:

FORENSICS:

-Identification of criminals: Collecting the evidence in the scene of crime.

-Surveillance: Using cameras one can monitor the very busy places such as stadiums, airport, meeting, etc.

-Corrections: This refers to the treatment of criminals through a system of rehabilitation or the administrative system by which these are effectuated.

-Probation and home arrest: Biometric can also be used for post – release programs to ensure the fulfilment of the probation, parole and home detention terms.

GOVERNMENT:

There are many application of biometry in government sector.

-National Identification Cards: The idea is to include digital biometric information in the national identification card.

-Voter Id and Elections: While the biometric national ID card is still in project, many countries have already used the biometry for the control of voting and voter registration for the national or regional elections.

-Driver's licenses: In many countries the driver license is also used as identification document, therefore it is important to prevent the duplicate emission of the driver license under different name.

-Employee Authentication: The government use of biometric for PC, network and data access is also important for security of building and protection of information.

-Commercial: Banking and financial services represent enormous growth areas for biometric technology with many deployments currently functioning and pilot project announced frequently. Some applications in this sector are:

-Account Access: The use of biometric for the access to the account in the bank allows keeping definitive and auditable records of account access by employees and customers.

ATMs:

The use of biometric in the ATM transaction allows more security.

-Online Banking: Internet based account access is already widely used in many places; the inclusion of biometric will make more secure this type of transactions from home.

-Physical access: The biometric is widely used for controlling the access to building or restricted areas.

-E – Commerce: Biometric e - commerce is the use of biometrics to verify the identity of individual conduction remote transaction for goods or services.

-Telephony Transaction: Voice-scan biometric can be used to make more secure telephone – based transactions.

HEALTH CARE:

The applications in this sector include the use of biometrics to identify or verify the identity of individuals interacting with a health – care entity or acting in the capacity of health – care employee or professional.

-PC/Network Access: The biometric are used to control a secure access of the employees to the hospital network, primarily in order to protect the patient information.

-Access to Personal Information: Using biometrics, the medical patient information may be stored on smart card or secure network, this will enable the access of the patients to their personal information.

-Patient Identification: In case of emergency, when a patient does not have identification document and is unable to communicate, biometric identification may be a good alternative to identify.

-Travel and Immigration: The applications in this sector includes the use of biometrics to identify or verify the identity of individuals interacting during the course of travel, with a travel or immigration entity or acting in the capacity of travel or immigration employee.

-Air Travel: Many airports use a biometric system in order to reduce the inspection processing time for authorized travellers.

-Border Crossing: The use of biometrics to control the travellers crossing the national or state border is increasing specially in regions with high volume of travellers or illegal immigrants.

-Employees Access: Several airports use biometric to control the physical access of employees to secure areas.

-Passports: Some countries issue passports with biometric information on a barcode or smart chips.

1.7Performance Measures

I.FAR (False Acceptance Rate)

II. FRR (False Rejection Rate)

III. FER (False Error Rate)

IV. EER (Equal Error Rate)

V. Accuracy

When the matching module is operating in a one-to-one comparison mode (it compares feature set from one finger with template from one finger), it gives a *match* or *non-match* decision depending on whether the comparison score exceeded the threshold or not, respectively. The matching module, operating in one-to-one comparison mode, can commit two types of errors:

(i) Mistaking feature set and template from two different fingers to be from the same finger (called *false match*)

(ii) Mistaking feature set and template from the same finger to be from two different fingers (called *false non-match*).

It is important to understand the difference between false match and false non-match error and the more commonly used *false acceptance* and *false rejection* errors. The false match and false non-match are errors of the matching module in one-to-one comparison mode while false acceptance and false rejection are the error rates associated with verification and identification processes and in fact their exact meaning is dependent upon the type of identity claim made by the user. For example, in applications with positive claim of identity (e.g., an access control system) a false match from the matching module results in the false acceptance of an impostor into the system, whereas a false non-match from the matching module causes the false rejection of a genuine user in the system. On the other hand, in an application with negative claim of identity (e.g., preventing users from obtaining welfare benefits under false identities), a false match from the matching module results in rejecting a genuine request, whereas a false non-match from the matching module results in falsely accepting an impostor request. Further, an application may use other criteria for acceptance/rejection in addition to match/non-match decision. The notion of "false match/false non-match" is not application dependent and therefore, in principle, is more appropriate than "false acceptance/false rejection". However, the use of false acceptance (and False Acceptance Rate, abbreviated as FAR) and false rejection (and False Rejection Rate, abbreviated as FRR) is more popular, especially in the commercial sector. We will try to avoid the use of false acceptance and false rejection; they are synonyms for false match and false non-match, respectively.

When a biometric system operates in the identification mode, matching module works in One-to-many comparison mode. In its simplest form, one-to-many comparison against *N* templates can be viewed as a series of *N* one-to-one comparisons. If identification is performed only for subjects who are present in the enrollment database, the identification is known as *closed-set identification*. Closed-set identification always returns a non-empty candidate list. While closed-set identification has been studied extensively by researchers, it is rarely used in practice. In *open-set identification,* some of the identification attempts are made by subjects who are not enrolled. In the rest of this book when we refer to identification we will focus only on the open-set scenario. If the matching module is given a feature set from finger A and a set of templates that includes at least one template of A, and the matching module produces an empty candidate list, the error is called a *false negative identification error*. If the matching module is given a feature set from finger A and a set of templates that does not include any template from A and the matching module returns a non-empty candidate list, the error is called a *false positive identification error*.

$$\text{error rate} = \frac{\text{number of misclassified fingerprints} \times 100}{\text{total number of fingerprints}}\%$$

$$\text{accuracy} = 100\% - \text{error rate}.$$

CHAPTER 2: BACKGROUND AND LITERATURE REVIEW

2.1Fingerprint Representation

The fingerprint pattern when analyzed at different scale inhibits different types of features:

I) Level 1

II) Level 2

III) Level 3

Level 1 At the global level, the ridge line flow delineates the pattern. Singular points, called loop and delta (denoted as squares and triangles respectively), act as the control points around which the ridge lines are wrapped. Singular points and coarse ridge line shape are useful for fingerprint classification and indexing, but their distinctiveness is not sufficient for accurate matching. External fingerprint shape, orientation image and the frequency image also belong to the set of features that can be detected at the global level. At the global level (Level 1), ridges often run smoothly in parallel but exhibit one or more regions where they assume distinctive shapes (characterized by high curvature, frequent ridge terminations, etc.). These regions, called *singularities* or *singular region* may be broadly classified into three typologies: *loop*, *delta*, and *whorl*. Singular regions belonging to loop, delta, and whorl types are typically characterized by ∩, Δ, and O shapes, respectively. Sometimes whorl singularities are not explicitly introduced because a whorl type can be described in terms of two loop singularities facing each other.

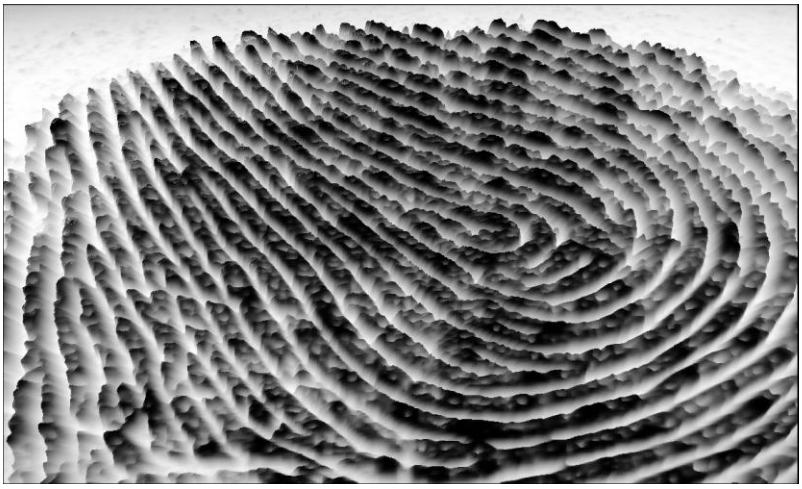


Figure 4 ridges and valley

Level 2 Minutiae are the most commonly used features in automatic fingerprint matching. Sir Francis Galton (1822−1911) was the first person to categorize minutiae and to observe that they remain unchanged over an individual's lifetime (Galton, 1892). Minutiae are sometimes called "Galton details" in his honor. At the local level, a total of 150 different local ridge characteristics, called minutiae details, have been identified. The local ridge characteristics are not evenly distributed. Most of them depend heavenly on the impression conditions and quality of fingerprints and are rarely observed in fingerprints. The two most prominent ridge characteristics are: 1) ridge endings and 2) ridge bifurcation.

1) Ridge Ending: It is a point where the ridge ends abruptly.

2) Ridge Bifurcation: It is a point where the ridge is divided into two branches. Minutiae in fingerprints are generally stable and robust to fingerprint impression conditions. Although a minutiae based representation is characterized by a high saliency, reliable automatic minutiae extraction can be problematic in low quality fingerprints devoid of any ridge structure.

Figure 5 given below shows a portion of the fingerprint image where the ridge lines appear as dark traces on a light background; two ridge endings and one bifurcation are shown.

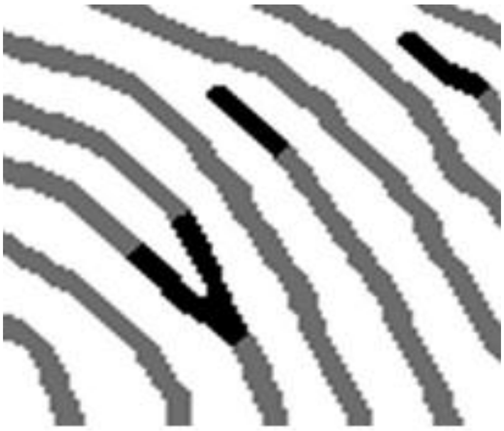


Figure 5 portion of the fingerprint image

Level 3 At this very fine level, intra ridge details can be detected. These include width, shape, curvature, edge contours of ridges as well as some other permanent details such as dots and incipient ridges. One of the finest level details is the finger sweat pores, whose positions and shapes are considered highly distinctive. However, extracting the very fine level details is feasible only in the high resolution fingerprint images of good quality and therefore this representation is not practical for non forensic applications. If the resolution is less than 1000 dots per pixel, then these details cannot be extracted. At local level, minutiae or small details mark the regions of local discontinuity within a fingerprint image. These are the locations where the ridge comes to an end or branches into two. Other forms of minutiae details include a very short ridge or a closed loop. There are more than 18 different type of minutiae among which the ridge endings and the bifurcations are most frequently used. A good quality fingerprint typically contains about 40-100 minutiae.

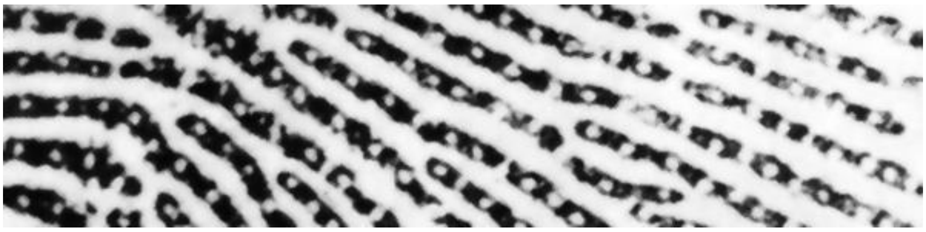


Figure 6: level 3 details like width, shape etc. of the pore

2.2Advantages of Minutiae Representation

i) Forensic experts also use minutiae representation to establish correspondence between two fingerprint images.

ii) Representation of minutiae information is covered by several standards such as ANSI-NIST and CBEFF making it necessary to use minutiae information if we want interoperability between two different algorithms.

iii) Minutiae based matching algorithms have accuracy comparable to sophisticated correlation based algorithms. However, while correlation based algorithms have large template sizes, minutiae based representation is very compact, seldom requiring more than 1 KB to store the template.

iv) Minutiae features have been historically proven to be distinctive between any two individuals and several theoretical models exists that provide a reasonable approximation of its individuality. No such models have been developed for texture based and image based descriptions.

v) Minutiae based representations contain only local information without relying on the global information such as singular points or centre of mass of fingerprints that are error prone and difficult to estimate accurately in poor quality images.

vi) Minutiae features are invariant to displacement and rotations unlike texture and image based features.

Pore Extraction

The appearance of a pore in a fingerprint image can differ in both shape and size due to its perspiration activity, as the pore may be open in one image and closed in another image (see Figure 3.6). On the other hand, pores appear only on the ridges and can be associated with the ridges already extracted. We propose to extract pores with regard to their central positions as well as their ridge ownership information.

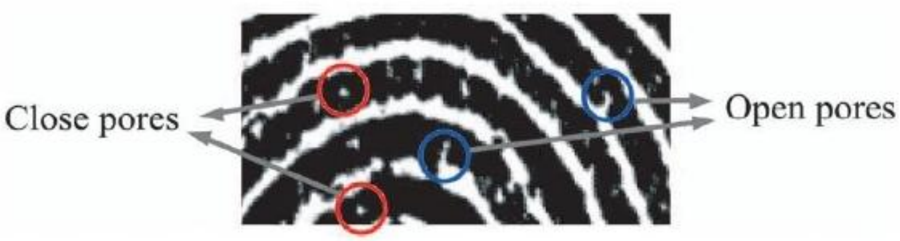


Figure 3.6: Appearance of pores. A pore can be open or closed due to its perspiration activity

Pores are extremely fine details which are lost after the enhancement stage. Therefore, for pore extraction the enhancement stage is omitted and pores are directly extracted from the pre processed image. The pore extraction algorithm can be broadly classified into two classes: the first class of algorithms extract pores by tracing fingerprint skeletons, the second class of algorithms extract pores directly from gray scale image. Stosz et al. and Kryszczuk et al. have proposed skeletonization based approach for pore extraction. The skeletonization based approach is reliable for extracting pores in good quality (and high resolution) images. As the image resolution decreases or the skin condition is not favorable, the method does not give reliable results. In Jain et al. have proposed a pore extraction technique directly from gray scale image. The majority of existing approaches for pore extraction consider only location information of pores for matching. The pores are distributed over ridges and using orientation detail can provide additional information for matching. A recent study by the International Biometric Group has proposed a new approach for pore extraction which utilizes orientation information of pores along with the location information. The approach proposed in is presented in this section. The first step in pore extraction process is the estimation of ridge orientation. This data is utilized later in the representation of pores. The Local Ridge orientation is determined by the least square estimate method. The fingerprint image is first divided into a number of non-overlapping blocks of dimension *w.w*. For each pixel (*i, j*) in the pre processed image, gradients in both the horizontal and vertical direction

2.3 Fingerprint Matching

A fingerprint matching algorithm compares two given fingerprints and returns either a degree of similarity (without loss of generality, a score between 0 and 1) or a binary decision (mated/non-mated). Only a few matching algorithms operate directly on grayscale fingerprint images; most of them require that an intermediate fingerprint representation be derived through a feature extraction stage. Without loss of generality, hereafter we denote the representation of the fingerprint acquired during enrollment as the *template* (T) and the representation of the fingerprint to be matched as the *input* (I). In case no feature extraction is performed, the fingerprint representation coincides with the grayscale fingerprint image itself; hence, we denote both raw fingerprint images and fingerprint feature vectors (e.g., minutiae) with T and I. The fingerprint feature extraction and matching algorithms are usually quite similar for both fingerprint verification and identification problems.

2.3.1 Fingerprint Matching Techniques

I) Correlation Based Technique:

In this type of matching, two fingerprint images are superimposed on each other and correlation between the corresponding pixels is computed for different alignment. Let T and I be the fingerprint images corresponding to the template.

T= template stored in the database.

I= Input fingerprint

Sum of square differences between the intensity of the corresponding pixels

$SSD\ (TI) = ||T-I||2 = ||T|| + ||I|| - 2TI$

Subscript T denotes the transpose of the vector.

Also we can compute the cross correlation of T, I

$CC\ (T, I) = TTI$

Cross Correlation= to compute the point of differences between the two fingerprint images.

Let (I (Δ x, Δ y, θ)) represents the input image I and angle theta be the Rotation around the origin, shifted by the displacements in the direction of x and y. then the similarity between two fingerprint images are:

$S\ (T, I) = \max\ (CC\ (T, I)$

But the underlying problems are:

i) Direct application of the correlation based matching is very expensive.

ii) Skin condition and finger pressure cause image brightness, contrast, and ridge thickness to vary significantly across different impressions. The use of more sophisticated correlation measures such as the normalized cross-correlation or the zero-mean normalized cross-correlation may compensate for contrast and brightness variations and applying a proper combination of enhancement, binarization, and thinning steps (performed on both **T** and **I**) may limit the ridge thickness problem. Hatano et al. proposed using the *differential correlation*, which is computed as the maximum correlation minus the minimum correlation, in a neighborhood of the point where the correlation is max. In fact, due to the cyclic nature of fingerprint patterns, if two corresponding portions of the same fingerprint are slightly misaligned with respect to their optimum matching position, the correlation value falls sharply whereas two non corresponding portions exhibit a flatter correlation value in the neighborhood of the optimum matching position. Hatano et al. (2002) reported a significant accuracy improvement with respect to the conventional correlation method.

ii) Minutiae Based Matching:

This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. In this type of matching, minutiae details are extracted from two fingerprints and stored as the set of points in the 2D space { it can also be stored in 3D space).Minutiae matching consists of finding the alignment between the template and the input minutiae set that result in the maximum number of minutiae pairing.

iii) Non minutiae Based Matching:

Minutiae extraction is difficult in the case of low quality fingerprint images whereas other features of fingerprint may be extracted more reliably. Feature extraction and template generation are based upon the series of ridges as opposed to discrete points which forms the basis of pattern matching techniques. The pattern of pattern matching over minutiae extraction is that minutiae points may be affected by wear and tear and the disadvantages are that these are sensitive to the proper displacement of finger and need large storage memory.

iv) Image Based Technique:

It is based on the global features of the whole fingerprint image. This is an advanced and new emerging method. Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Image based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centres on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

CHAPTER 3 PROPOSED WORK

3.1 System Design

3.1.1System Level Design

A fingerprint recognition system constitutes of fingerprint acquiring device, minutia extractor and minutia matcher [Figure 3.1.1].

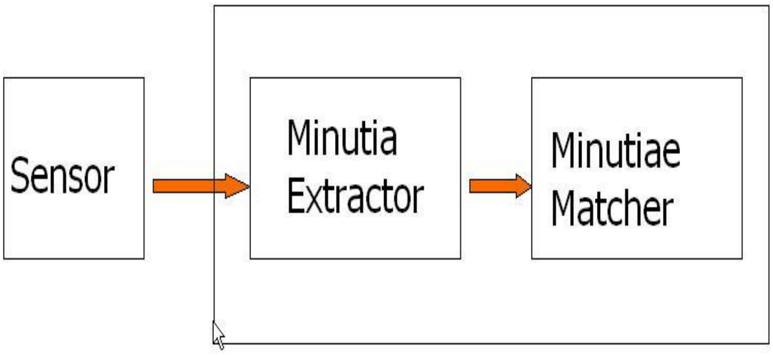


Figure 3.1.1 Simplified Fingerprint Recognition System

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 my project is from the available fingerprints provided by FVC2002 (Fingerprint Verification Competition 2002). So no acquisition stage is implemented.

The minutia extractor and minutia matcher modules are explained in detail in the next part for algorithm design and other subsequent sections.

3.1.2Algorithm 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 [Figure 3.2.1].

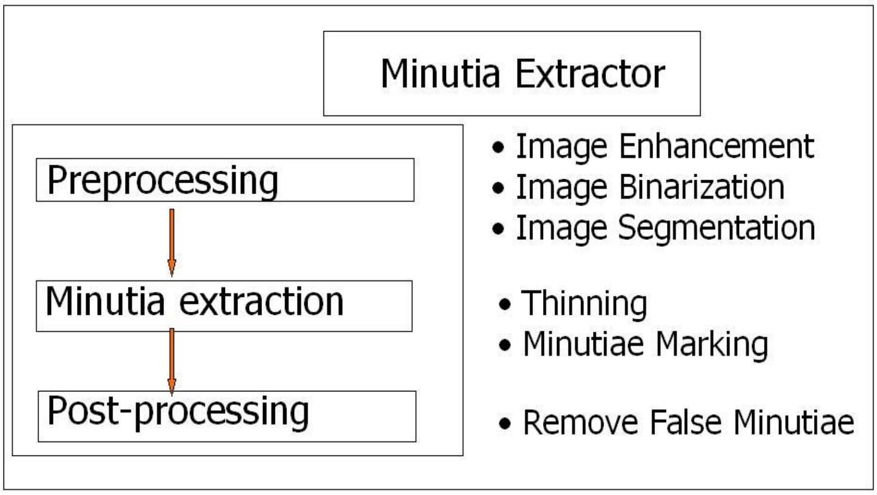
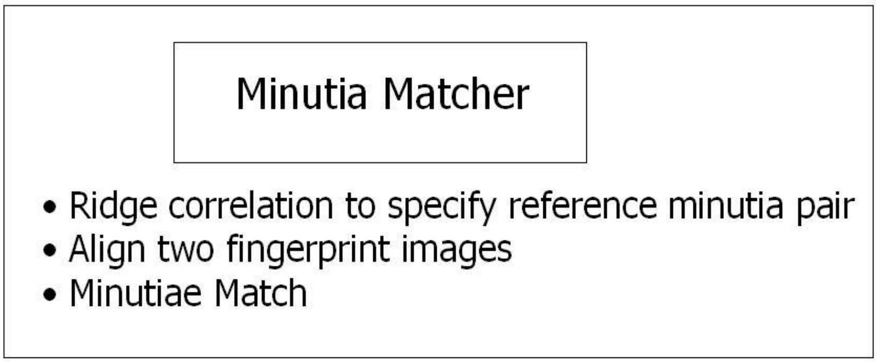


Figure 3.2.1 Minutia Extractor

For the fingerprint image preprocessing stage, we can use Histogram Equalization and Fourier Transform 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. Most methods used in the preprocessing stage are developed by other researchers but they form a brand new combination in my project through trial and error. Also the morphological operations for extraction ROI are introduced to fingerprint image segmentation by me.

For minutia extraction stage, three thinning algorithms are tested and the Morphological thinning operation is finally bid out with high efficiency and pretty good thinning quality. The minutia marking is a simple task as most literatures reported but one special case is found during my implementation and an additional check mechanism is enforced to avoid such kind of oversight.

For the post processing stage, a more rigorous algorithm is developed to remove false minutia based on. Also a novel representation for bifurcations is proposed to unify terminations and bifurcations.

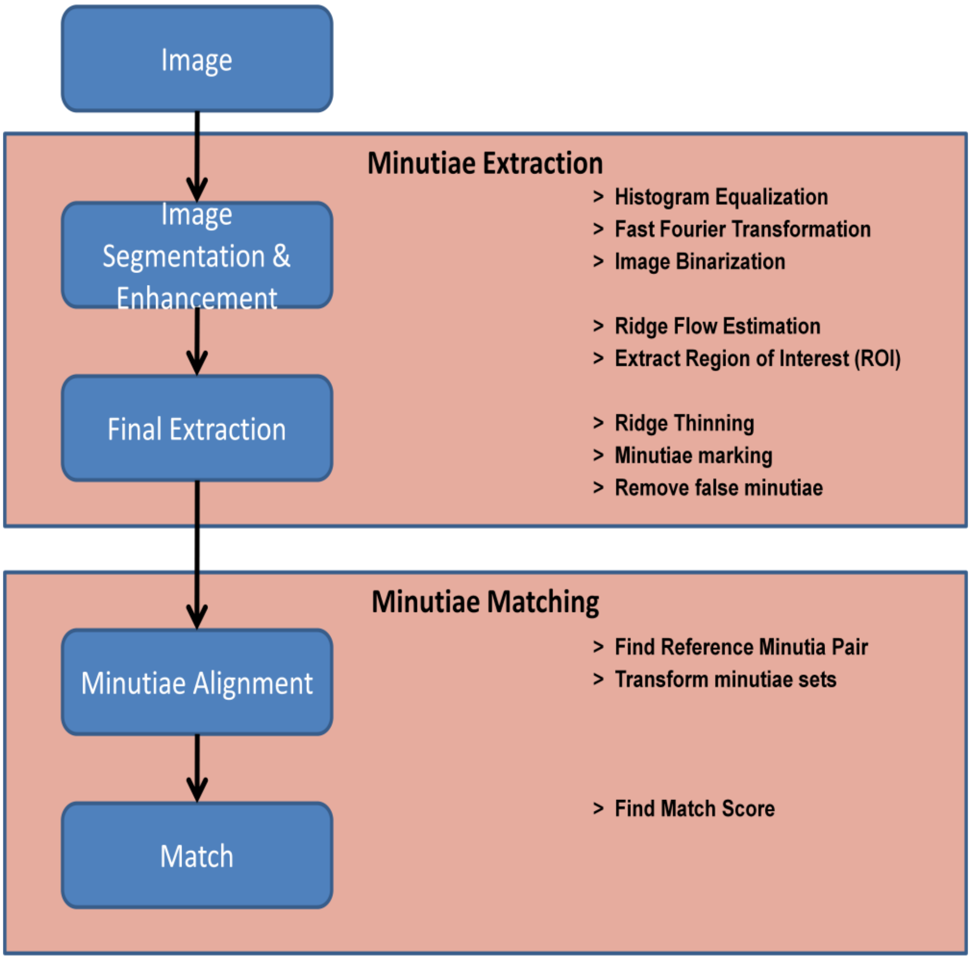


Minutia Matcher

- Ridge correlation to specify reference minutia pair
- Align two fingerprint images
- Minutiae Match

Figure3.2.2 Minutia Matcher

The minutiae matcher chooses any two minutiae as a reference minutiae pair and then matches their associated ridges first. If the ridges match well, two fingerprint images are aligned and matching is conducted for all remaining minutia [Figure 3.2.2].



3.2 Minutiae Extraction

As described earlier the Minutiae extraction process includes image enhancement and final Minutiae extraction.

3.2.1Fingerprint Image Enhancement

The first step in the minutiae extraction stage is Fingerprint Image enhancement. This is mainly done to improve the image quality and to make it clearer for further operations. Often fingerprint images from various sources lack sufficient contrast and clarity. Hence image enhancement is necessary and a major challenge in all fingerprint techniques to improve the accuracy of matching. It increases the contrast between ridges and furrows and connects the some of the false broken points of ridges due to insufficient amount of ink or poor quality of sensor input. Fingerprint Image enhancement is to make the image clearer for easy further operations. Since the fingerprint images acquired from sensors or other Medias are not assured with perfect quality, those enhancement methods, for increasing the contrast between ridges and furrows 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.

In our project we have implemented two techniques: Histogram Equalization and Image Binarization.

Histogram Equalization:

Histogram equalization is a technique of improving the global contrast of an image by adjusting the intensity distribution on a histogram. This allows areas of lower local contrast to gain a higher contrast without affecting the global contrast. Histogram equalization accomplishes this by effectively spreading out the most frequent intensity values. Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. The original histogram of a fingerprint image has the bimodal type [Figure 3.2.1.1], the histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced [Figure 3.2.1.1].

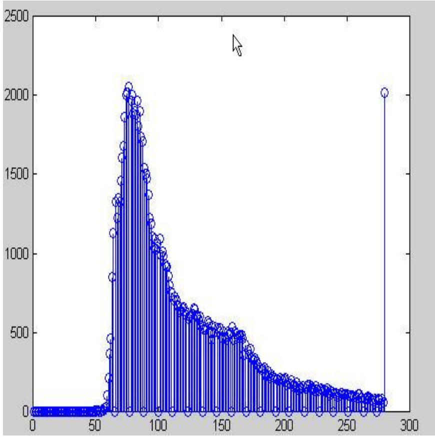


Figure3.2.1.1 the Original histogram of a fingerprint image

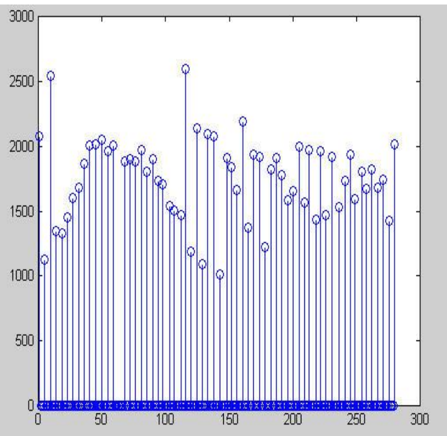


Figure 3.2.1.2 Histogram after the Histogram Equalization

The right side of the following figure [Figure 3.2.1.3] is the output after the histogram equalization.

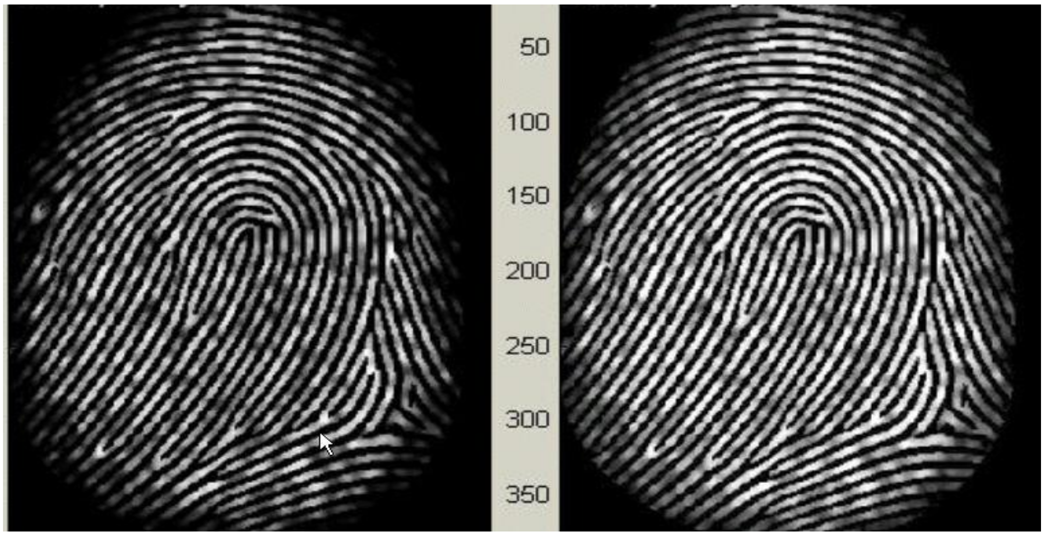


Figure: 3.2.1.3 Histogram Enhancement.

Original image (Left). Enhanced image (Right)

Fourier transform:-

Here first of all we divide the image into different small processing blocks those are of 32 by 32 pixels then use the Fourier transform. To enhance those small processing blocks through its dominant frequencies, we multiplied the FFT of the block with its magnitude a set of times. Where the magnitude of the original FFT = abs (F (u, v)) = |F (u, v)|. Now we get the enhanced block according to the formula:-

$$G(x, y) = F^{-1}\{F(u, v) * |F(u, v)|^{k}\}$$

K is an experimentally determined constant used in equation, where we have taken the value of k=0.45 for the further calculation. If the value of "k" increases then the appearance of the ridges also increases and it is filling up small holes in ridges, if the value of "k" is too high then it may results false joining of ridges. Thus a termination might become a bifurcation. The given figure presents the image after FFT enhancement.

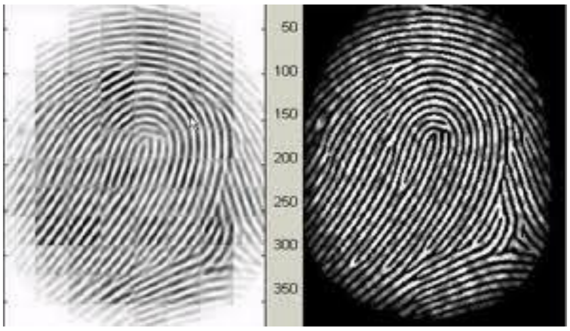


Figure 13

Original Image Fingerprint Enhanced by FFT

After the enhancement of the image through FFT it is quite easy to connect the falsely broken points on ridges and it becomes simpler to remove some unwanted cross connections between ridges.

Fingerprint Image Binarization

Fingerprint Image Binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows are white.

A locally adaptive binarization method is performed to binarize the fingerprint image. Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs [Figure 4.2.1].

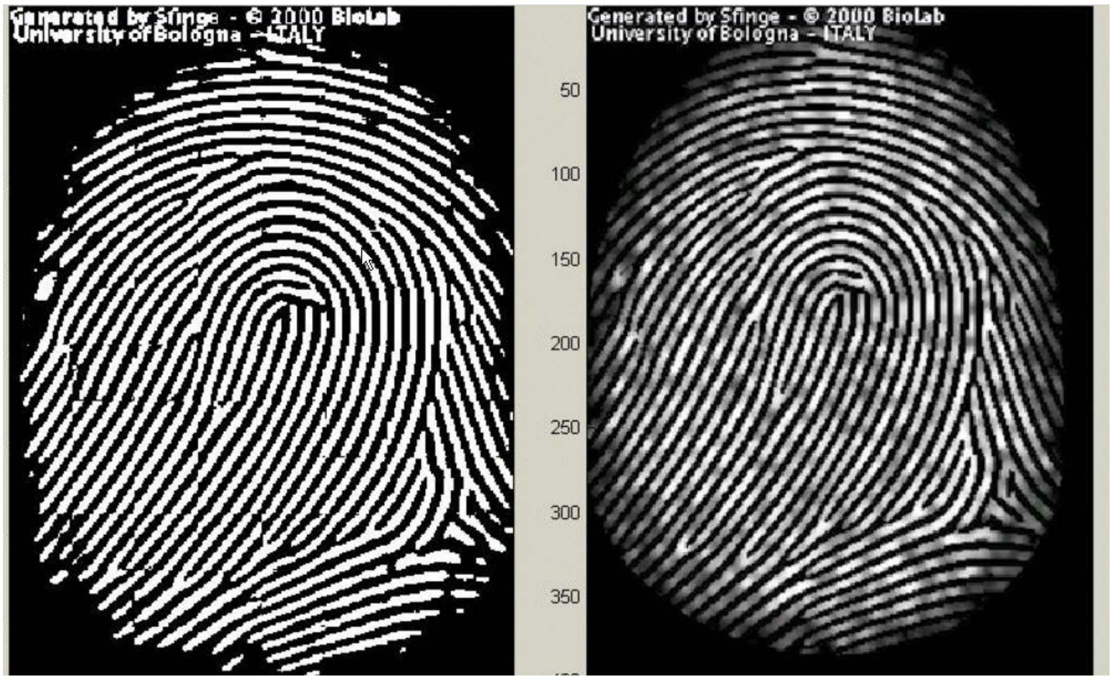

Generated by Sfinge - © 2000 Biolab
University of Bologna - ITALY
50
100
150
200
250
300
350
Generated by Sfinge - © 2000 BioLab
University of Bologna - ITALY

Figure: 4.2.1 the Fingerprint image after adaptive binarization

Binarized image Enhanced gray image

Fingerprint Image Segmentation

In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information. Then the bound of the remaining effective area is sketched out since the minutia in the bound region is confusing with that spurious minutia that is 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 [1], while the second is intrigued from some Morphological methods.

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 is:

i) Calculate 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, use following formula to get the Least Square approximation of the block direction.

$tg2ß = 2 \sum \sum (g_x*g_y)/\sum \sum (g_x^2-g_y^2)$ 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.

$tg2\theta = 2\sin\theta \cos\theta / (\cos^2\theta - \sin^2\theta)$

After finished with the estimation of each block direction, those blocks without significant information on ridges and furrows 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.

The direction map is shown in the following diagram. We assume there is only one fingerprint in each image.

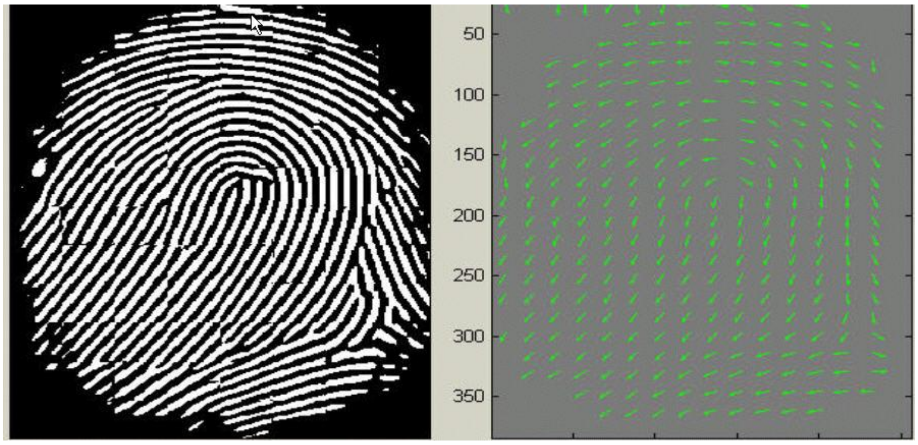


Figure 3.3.1.1 Direction map.

Binarized fingerprint (left), Direction map (right)

1. ROI extraction by Morphological operations

Two Morphological operations called ‘OPEN’ and ‘CLOSE’ are adopted. The ‘OPEN’ operation can expand images and remove peaks introduced by background noise. The ‘CLOSE’ operation can shrink images and eliminate small cavities

3.2.2Final minutiae Extraction

After completing the enhancement and binarization process now our job is to extract the minutiae of the fingerprint image. The minutia extraction stage is divided in to two sub stages such as i) Ridge Thinning and ii) Minutiae Marking

Fingerprint Ridge Thinning

The ridge thinning process is used to eliminate the redundant pixels of ridges till the ridges are just up to one pixel wide. This is done by using the following MATLAB‟s thinning function.

Bwmorph (binary_image,’thin‟, Inf)

Then the thinned image is filtered by using the following three MATLAB‟s functions. This is used to remove some H breaks, isolated points and spikes.

Bwmorph (binaryImage, “hbreak”, k)

Bwmorph (binaryImage, “clean”, k)

Bwmorph (binaryImage, “spur”, k)

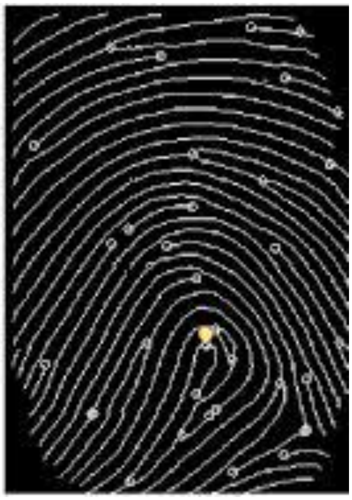


IMAGE BEFORE THINNING IMAGE AFTER THINNING

Minutiae marking

After completion of fingerprint ridge thinning, minutiae marking are done by using 3x3 pixel windows. In case of minutia marking the concept of Crossing Number (CN) is mainly used.

POST PROCESSING IMAGE:

This stage includes two sub stages such as:

i) false minutia removal
ii) unify termination bifurcation

False Minutia Removal

The pre - processing stage can’t completely heal the fingerprint image. At this stage different types of false minutia are generated due to insufficient amount of ink or excess inking. False ridge breaks generated due to insufficient ink and the cross connection between the ridges occurs due to over inking. Some of the previous techniques also introduce some spurious minutia points in that image. These types of false minutia are not totally eliminated. So to make the fingerprint recognition system consistent we have to remove all types of false minutia. Here first of all we have to calculate the inter ridge distance (D) which is the average distance between two neighbouring ridges. By using the following formula we can calculate the inter ridge distance (D) easily.

Inter ridge distance = (Sum of all pixels with value 1/row length)

Finally an averaged value over all rows gives D.

Unify termination and bifurcation:-

We know one type of minutia can be change to other type easily, coming in contact with the different types of data acquisition conditions. So we have to save them in some form of representation that is both for termination and bifurcation. So each minutia is completely characterized by the following parameters at last:

1) x-coordinate

2) y-coordinate

3) Orientation.

4) Associated ridge

Actually a bifurcation can be broken down to three terminations each having their own x-y coordinates, orientation and an associated ridge. The orientation for each termination (tx, ty) is estimated by using the following method.

i) First of all we have to track a ridge segment, whose starting point must be the termination and length is D.
ii) Then sum up all the x-coordinates of points present in that particular ridge segment.
iii) After that to get Sx we have to divide the above summation with D and sequentially we get Sy using the same technique.

Now we can get the direction from the expression:

Tan^-1((sy-ty)/ (sx-tx))

RESULT AFTER MINUTIAE EXTRACTION STAGE

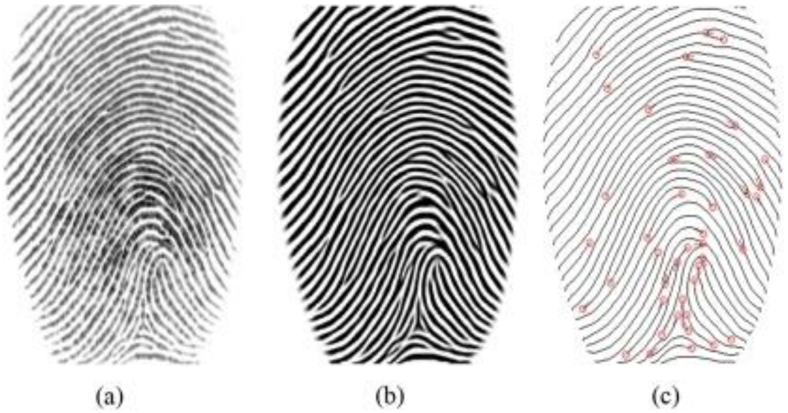


Figure 1

THINNED IMAGE AFTER MINUTIA MARKING AFTER REMOVAL OF FALSE MINUTIA

3.3 Minutiae Matching

The minutia details of two fingerprints are obtained using the above procedures and they are matched using the minutia match algorithm. It comprises of two stages:

1) Alignment stage

2) Match stage

An iterative ridge alignment algorithm is first used to align one set of minutia with respect to another and then an elastic match algorithm is carried out to count the number of matching minutia pairs.

MINUTIAE ALIGNMENT

1) Let I1 and I2 represent two set of minutiae given by

I1 = {m1, m2, m3 ...mn} where mi= {xi, yi, θi}

I2 = {m1', m2', m3' ...mN'} where mi'= {xi', yi', θi'}

One minutia from each set is chosen and the ridge correlation factor is calculated in between them. The ridges associated with each minutia are represented by a series of x-coordinates (x1, x2, x3, x4, xn) of the points on the ridges. Sampling is done per ridge length L from the starting of the minutia point where L is the average inter ridge width and n is set to 10 unless total ridge length is less than that of 10*L.

So the similarity of correlating the two ridges is derived from:

$$S = \sqrt{\frac{\sum_{i=0}^{m} xiXi}{\sum_{i=0}^{m} xi^2 Xi^2}}$$

Where (x_i...x_n) and (X_i...X_n) are the set of x-coordinates for each of the 2 minutia chosen. And m is minimal one of the n and N value. If the similarity score is larger than 0.8, then go to step 2, otherwise continue to match the next pair of ridges. Where (x1,x2,x3,...,xn) and (X1,X2,X3,...,Xn) represents two sets of x-coordinates for 2 minutia chosen and m is one of the minimal value of n and N. If the similarity score is above 0.8 then go to step 2 otherwise continue the process of matching for next 2 minutiae.

2) In the second stage each set of minutia is transformed with respect to the reference minutia and then matched in a unified x-y coordinate.

Suppose M(x, y, θ) be the reference minutia derived from step 1(say from I1). Then for each minutia, translation and rotation of all other minutiae is done with respect to the reference minutiae M.

$$\begin{pmatrix} xi\_new \\ yi\_new \\ \theta i\_new \end{pmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} xi - x \\ yi - y \\ \theta i - \theta \end{bmatrix}$$

The new coordinate system is originated at reference minutia M and the new x-axis is coincident with the direction of minutia M. No scaling effect is taken into account by assuming two fingerprints from the same finger have nearly the same size. So we get transformed sets of minutiae I_1' & I_2'.

Minutiae Match

An elastic string $(x, y\ \theta)$ match algorithm is used to find number of matched minutia pairs among I_1' & I_2'.

According to the elastic string match algorithm minutia m_i in I_1' and a minutia m_j in I_2' are considered "matching," if the spatial distance (sd) between them is smaller than a given tolerance r_0 and the direction difference (dd) between them is smaller than an angular tolerance Θ_0.

$$\text{sd} = \sqrt{(xi - xj)^2 + \ (yi - yj)^2} \leq r_0$$

$$\text{dd} = \min\ \ (|\theta i - \theta j|, 360 - |\theta i - \theta j|) \leq \Theta_0$$

Let mm (.) be an indicator function that returns 1 in the case where the minutiae m_i and m_j match according to above equations.

$$\text{mm}\ (m_i,m_j)= \begin{cases} 1, & sd(m_i, m_j) \leq r_0 \text{and dd}(m_i, m_j) \leq \theta_0 \\ 0, & otherwise \end{cases}$$

Now the total number of matched minutiae pair given by,

$$\text{num (matched minutiae)} = \sum \text{mm}(m_i, m_j)$$

and final match score is given by,

$$\text{Match Score} = \frac{num\ (matc\,hed\ minutiae\ )}{\max(num\ of\ minutiae\ \ in\ I_1, I_2\ )}$$

Steps involved in fingerprint recognition system:

As an emerging biometric identification technology, fingerprint identification technology has become quite a prevalent force in the industry. Our current market contains various fingerprint identification devices. The identification process is mainly comprised of following steps: pre-processing, feature extraction, matching, and identification. Fingerprint image pre-processing can be detailed into image enhancement, binarization and thinning.

i)Image pre-processing:. The purpose of pre-processing is to remove the noise in image, change the image to a clear figure chart with obvious edges, in order to extract correct features. Fingerprint image pre-processing is one of the most important steps of the entire identification process, because its results have a direct impact on the success of identification.

ii) Image enhancement: The most important step in pre-processing stage is to enhance the fingerprint image. Its purpose is to enhance the structural contrast of ridges and valleys while inhibiting noise, connect broken ridges as well as separate attached ridges, highlight information in the image according to specific requirements, and weaken or remove those unnecessary pieces of information.

iii) Binarization: After the image enhancing treatment, the lines (ridges) in image are enhanced. However, the intensities of ridges are unique, and have different grey scales. The purpose of binarization is to unify the grey scales so the image is able to be simplified into binary information. It also separates attached ridges and makes provisions for feature exaction and matching.

iv) Thinning: After binarization, ridges are still of certain width. However, fingerprint identification software only requires the direction of these ridges. The purpose of thinning is to remove the pixels on ridge edges, and to keep ridges within one pixel. This is to remove redundant information and highlight the main features in order to facilitate exaction.

v) Feature extraction: There are two exaction methods: one method is to extract from the grey scale image, and the other is to extract from a thinned binary image. The algorithm that directly extracts features from grey scale image usually tracks the grey scale ridges and finds the locations of features, determining the types of features based on the tracking result.

vi)Matching and identification**:** This is the last step in the fingerprint identification system, as well as the biggest factor for evaluating the performance of the fingerprint identification system. Fingerprint matching uses the extracted features to determine whether two fingerprints are from the same finger. Feature matching is a process that matches the minute features of a newly input fingerprint to those stored in the fingerprint database and locates the most identical fingerprint as the output. Matching is the ultimate purpose of the fingerprint identification system. Due to multiple influencing factors, the same fingerprint may match different feature templates. Though there is always going to be some margin of error, it is small enough for us to accurately match fingerprints.

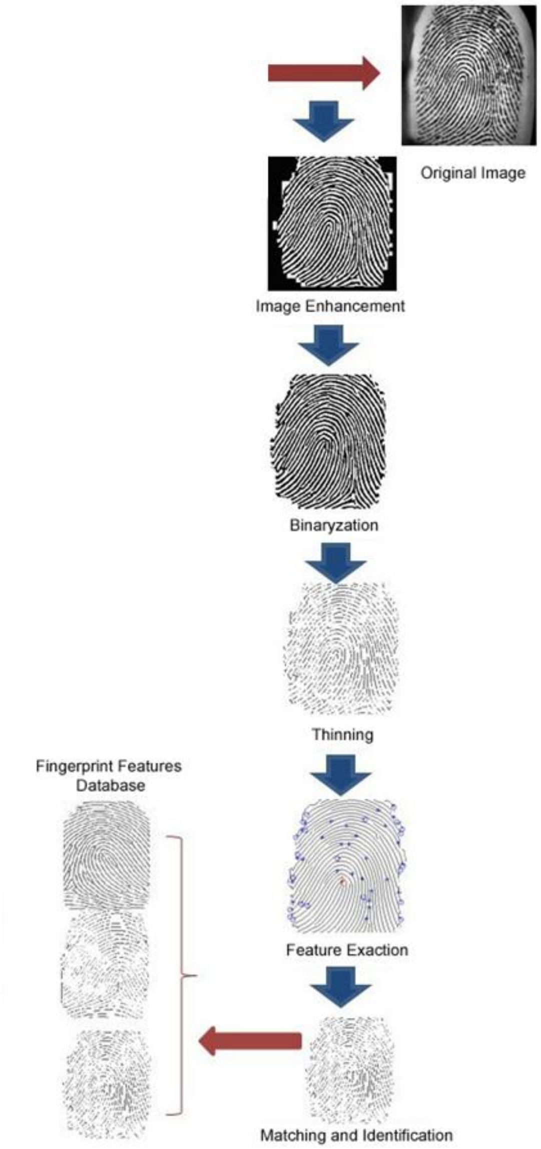


Figure 2 Process Chart of Fingerprint Identification System

The fingerprint image matching algorithm required for matching and identification of fingerprint features is usually divided into one-to-one verification and one-to-many identification.

The former is a verification process which uses a person's ID to first get his/her fingerprint features from the fingerprint database, then match them with the features of the newly acquired fingerprint, so as to identify the person.

The latter is an identification process which first extracts the features of the newly acquired fingerprint, then matches those features to those stored in fingerprint database one by one, so as to identify the person.

3.4 Algorithm:

Input: Take Fingerprint images from fingerprint reader.

Output: Generate matching score of fingerprints and produce performance of fingerprint recognition system.

Step 1: Receive fingerprint images from fingerprint reader and image will supply to FRS
As input.

Step 2: Apply basic pre-processing steps like Binarization and Thinning for image enhancement.

Step 3: Mark minutiae points (Ridges-end point and bifurcation point) and extract all the
Information about fingerprint image.

Step 4: Finally fingerprint matching Step occur.

In this we have two conditions:

(a) First condition: where Imposter user will apply to the system, when the fingerprint
Is accepted or not then the information is updated in FAR table.

(b) Second condition: where genuine user will apply, then if the fingerprint is rejected or
Accepted then information goes in FRR.

CHAPTER 4 EXPERIMENTAL RESULT

4.1Performance Evaluation Index

Two indexes are well accepted to determine the performance of a fingerprint recognition system:

i) False Rejection Rate (FRR)**:** For an image database, each sample is matched against the remaining samples of the same finger to compute the False Rejection Rate

ii) False Acceptance Rate (FAR): Also the first sample of each finger in the database is matched against the first sample of the remaining fingers to compute the False Acceptance Rate.

4.2Experiment Analysis

The evaluations and testing of the proposed approach has been done on three diverse fingerprint databases: FVC2002, FVC2004 DB3 Database and FVC2006 DB2 Database. They are explained in detail below.

I) FVC 2002*:* A fingerprint database from the FVC2002 (Fingerprint Verification Competition 2002) is used to test the program's performance. A series of correct and incorrect match score is recorded. The relatively low percentage of verification rate is due to poor quality of images in the database and the inefficient matching algorithm which lead to incorrect matches.

Ii) FVC 2004 DB3 Database: The database consists of 100 different fingers with 8 impressions per finger resulting in 800 images. The fingerprints are scanned with a thermal sweeping sensor (Finger Chip FCD4B14CB by Atmel) at 512 dpi. The FVC 2004 databases are known to be difficult because of the perturbations which were deliberately introduced during database collection. The sample images from this database are shown in Figure 4.1.

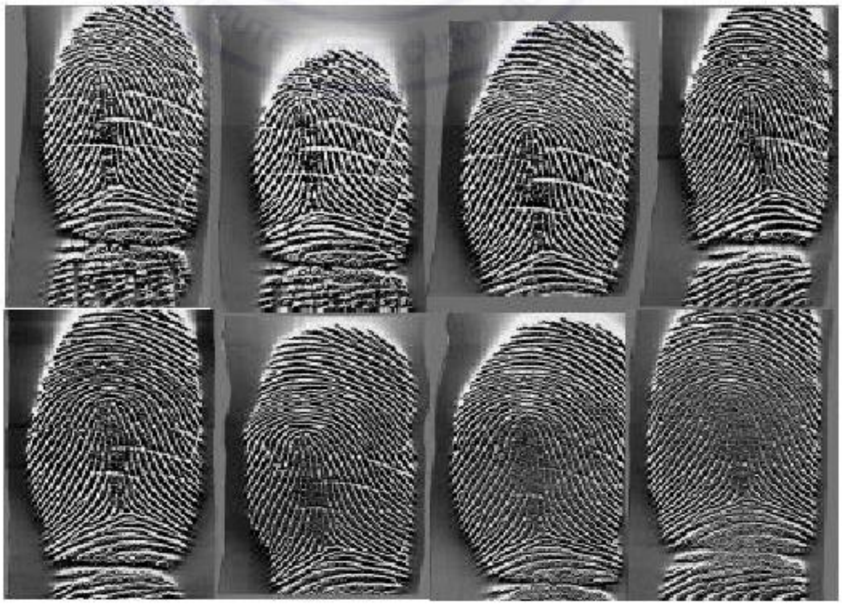


Figure 4.1: Sample images from FVC2004, DB3 Database

Iii) FVC 2006 DB2 Database: The database is 140 fingers wide and 12 samples per finger in depth (total 1680 fingerprint). The fingerprints were scanned with an optical sensor at 569 dpi. A heterogeneous population which includes manual workers and elderly people was used to create the database. The volunteers were simply asked to put their fingers naturally on the acquisition device, but no constraints were enforced to guarantee a minimum quality in the acquired images. Figure 4.2 displays the sample images from this database.

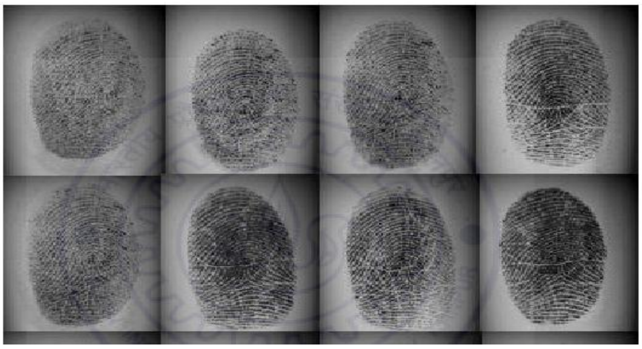


Figure 4.2: Sample images from FVC 2006, DB2 Database

CONCLUSION

The above implementation was an effort to understand how Fingerprint Recognition is used as a form of biometric to recognize identities of human beings. It includes all the stages from minutiae extraction from fingerprints to minutiae matching which generates a match score. Various standard techniques are used in the intermediate stages of processing.

The relatively low percentage of verification rate as compared to other forms of biometrics indicates that the algorithm used is not very robust and is vulnerable to effects like scaling and elastic deformations. Various new techniques and algorithm have been found out which give better results.

Also a major challenge in Fingerprint recognition lies in the pre processing of the bad quality of fingerprint images which also add to the low verification rate. The reliability of any automatic fingerprint system strongly relies on the precision obtained in the minutia extraction process. A number of factors damage the correct location of minutia. Among them, poor image quality is the one with most influence. There is a scope of further improvement in terms of efficiency and accuracy which can be achieved 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.

The hardware part is not illustrated here but the algorithm and basic concept behind each step are given with a priority study concept. And all the algorithms are coded using MATLAB.

REFERENCES

1. A. K. Jain,”Handbook of Fingerprint Recognition”, Department of Computer Science Michigan State University, USA.
2. A. K. Jain, “Introduction to Biometrics”, Department of Computer Science Michigan State University, USA.
3. Prof. S.Meher, “Study of Fingerprint Recognition System”, National Institute of Technology, Rourkela.
4. Manveet Kaur, “Fingerprint Verification System using Minutia Extraction Techniques”, World Academy of Science, Engineering and Technology.
5. Lin Hong. "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.
6. Lee, C.J., and Wang, S.D.: Fingerprint feature extraction using Gabor filters, Electron.
7. L. Hong, "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998
8. P. Komarinski, P. T. Higgins, and K. M. Higgins, K. Fox Lisa , “Automated Fingerprint Identification Systems (AFIS)”, Elsevier Academic Press, pp. 1-118, 2005.
9. Lin Hong, Student Member, IEEE, Yifei Wan, and Anil Jain, “Fingerprint Image Enhancement: Algorithm and Performance Evaluation” IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 20, pp. 777-787, 1998.
10. Lee et al. (2006). Lee C., Lee S., Kim J. and Kim S.J., “Pre-processing of a Fingerprint Image Captured with a Mobile Camera,” in *Proc. Int. Conf. on Biometrics*, LNCS 3832, pp. 348–355, 2006.
11. Asai et al. (1975). Asai K., Hoshino Y., Yamashita N. and Hiratsuka S., “Fingerprint Identification System,” in *Proc. Int. Conf. US–Japan Computer (2nd)*, pp. 30–35, 1975.
12. Champod and Margot (1996). Champod C. and Margot P.A., “Computer assisted analysis of minutiae occurrences on fingerprints,” in *Proc. Int. Symposium on Fingerprint Detection and Identification*, J. Almog and E. Spinger (Eds.), Israel National Police, Jerusalem, pp. 305, 1996.

13. Chen and Dong (2006). Chen H. and Dong G., "Fingerprint Image Enhancement by Diffusion Processes," in *Proc. Int. Conf. on Image Processing,* pp. 297–300, 2006.
14. Chen et al. (2004). Chen X., Tian J., Cheng J. and Yang X., "Segmentation of fingerprint images using linear classifier," *EURASIP Journal on Applied Signal Processing,* vol. 2004, no. 4, pp. 480–494,2004.Moenssens (1971).
15. Moenssens A., *Fingerprint Techniques,* Chilton Book Company, London, 1971.
16. L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," *IEEE Trans. Pattern Analysis and Machine Intelligence,* 1998.
17. J. P. Campbell, L. A. Alyea, and J. S. Dunn, "Biometric security: Government applications and operations," *http://www.biometrics.org/,* 1996.
18. Zhu, Yin and Zhang (2005). Zhu E., Yin J. and Zhang G., "Fingerprint matching based on global alignment of multiple reference minutiae," *Pattern Recognition,* vol. 38, no. 10, pp. 1685–1694,2005.
19. Handbook of Fingerprint Recognition by A. K. Jain
20. Introduction to Biometric by A. K. Jain
21. bias.csr.unibo.it/fvc2000/
22. bias.csr.unibo.it/fvc2004/
23. ieeexplore.ieee.org/
24. http://en.wikipedia.org/wiki/Biometrics
25. http://en.wikipedia.org/wiki/Fingerprint_Verification_Competition
26. http://www.biometrics.gov/documents/fingerprintrec.pdf

CODE IMPLEMENTATION

FEATURE EXTRACTION

```
%Program for Fingerprint Feature Extraction

%Program Description
%this program extracts the ridges and bifurcation from a fingerprint image

%Read Input Image
binary_image=im2bw (imread ('finger.tif'));

%Small region is taken to show output clear
binary_image = binary_image (120:400, 20:250);
Figure; imshow (binary_image); title ('Input image');

%Thinning
thin_image=~bwmorph (binary_image,'thin', INF);
Figure; imshow (thin_image); title ('Thinned Image');

%Minutiae extraction
s=size (thin_image);
N=3; %window size
n= (N-1)/2;
r=s (1) +2*n;
c=s (2) +2*n;
Double temp(r, c);
Temp=zeros(r, c); bifurcation=zeros(r, c); ridge=zeros(r, c);
Temp ((n+1) :( end-n), (n+1) :( end-n)) =thin_image (:,:);
OutImg=zeros(r, c, 3); %For Display
OutImg (: 1) = temp.* 255;
OutImg (:,:,2) = temp .* 255;
OutImg (: 3) = temp.* 255;
For x= (n+1+10) :( s (1) +n-10)
    For y= (n+1+10) :( s (2) +n-10)
        e=1;
        For k=x-n: x+n
            f=1;
            For l=y-n: y+n
                Mat (e, f) =temp (k, l);
                f=f+1;
            End
            e=e+1;
        End;
         If (mats (2, 2) ==0)
            Ridge(x, y) =sum (sum (~mat));
            Bifurcation(x, y) =sum (sum (~mat));
         End
    End;
End;

% RIDGE END FINDING
[ridge_x ridge_y]=find (ridge==2);
Len=length (ridge_x);
%for Display
For i=1: len
    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)-3),2:3)=0;
    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)+3),2:3)=0;
    outImg((ridge_x(i)-3),(ridge_y(i)-3):(ridge_y(i)+3),2:3)=0;
    outImg((ridge_x(i)+3),(ridge_y(i)-3):(ridge_y(i)+3),2:3)=0;

    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)-3),1)=255;
    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)+3),1)=255;
    outImg((ridge_x(i)-3),(ridge_y(i)-3):(ridge_y(i)+3),1)=255;
    outImg((ridge_x(i)+3),(ridge_y(i)-3):(ridge_y(i)+3),1)=255;
End

%BIFURCATION FINDING
[bifurcation_x bifurcation_y]=find (bifurcation==4);
Len=length (bifurcation_x);
%for Display
For i=1: len
    outImg((bifurcation_x(i)-3):(bifurcation_x(i)+3),(bifurcation_y(i)-3),1:2)=0;
    outImg((bifurcation_x(i)-3):(bifurcation_x(i)+3),(bifurcation_y(i)+3),1:2)=0;
    outImg((bifurcation_x(i)-3),(bifurcation_y(i)-3):(bifurcation_y(i)+3),1:2)=0;
    outImg((bifurcation_x(i)+3),(bifurcation_y(i)-3):(bifurcation_y(i)+3),1:2)=0;

    outImg((bifurcation_x(i)-3):(bifurcation_x(i)+3),(bifurcation_y(i)-3),3)=255;
    outImg((bifurcation_x(i)-3):(bifurcation_x(i)+3),(bifurcation_y(i)+3),3)=255;
    outImg((bifurcation_x(i)-3),(bifurcation_y(i)-3):(bifurcation_y(i)+3),3)=255;
    outImg((bifurcation_x(i)+3),(bifurcation_y(i)-3):(bifurcation_y(i)+3),3)=255;
End
Figure; imshow (outImg); title ('Minutiae');
```

Using this code, Fingerprint Minutiae points are extracted involving ridge end and bifurcation findings.

IMAGE ENHANCEMENT

```
Clear all
Clc
I=imread ('finger.tif');
I=double (I);
maximum_value=max ((max (I)));
[Row col]=size (I);
c=row*col;
h=zeros (1,300);
z=zeros (1,300);
For n=1: row
   For m=1: col
      If I (n, m) == 0
         I (n, m) =1;
      End
   End
End
For n=1: row
   For m=1: col
      t = I (n, m);
      H (t) = h (t) + 1;
   End
End
Pdf = h/c;
Cdf (1) = pdf (1);
For x=2:maximum_value
Cdf(x) = pdf(x) + cdf(x-1);
End
New = round (cdf * maximum_value);
New= new + 1;
For p=1: row

   For q=1: col
 Temp=I (p, q);
      B (p, q) =new (temp);
      t=b (p, q);
      Z (t) =z (t) +1;
   End
End
b=b-1;
Subplot (2, 2, 1), imshow (uint8 (I)), title ('Image1');
Subplot (2, 2, 2), bar (h), title ('Histogram of d Orig. Image');
subplot(2,2,3), imshow(uint8(b)) , title('Image2'); subplot(2,2,4),bar(z) , title('Histogram Equalization of image2');
```

Here, an input image is enhanced using one of the image enhancement technique i.e. Histogram Equalization.

Matching

```
Clc;
Clear all;
Close all;

pic1 = imread ('finger.tif');
pic2 = imread ('finger.tif');

Figure
Subplot (1, 2, 1);
Imshow (pic1)
Subplot (1, 2, 2);
Imshow (pic2)

%so that we obtain white and black points and edges of the objects present
%in the picture.

edge_det_pic1 = edge (pic1,'prewitt'); %applying edge detection on first picture


%so that we obtain white and black points and edges of the objects present
%in the picture.

edge_det_pic2 = edge (pic2,'prewitt'); %%applying edge detection on second picture
Figure
Subplot (1, 2, 1);
Imshow (edge_det_pic1)
Subplot (1, 2, 2);
Imshow (edge_det_pic2)
```

```
OUTPUT_MESSAGE = ' Hence the pictures have been matched, SAME PICTURES ';

OUTPUT_MESSAGE2 = ' Hence the pictures have not been matched, DIFFERENT PICTURES ';

%initialization of different variables used
matched_data = 0;
white_points = 0;
black_points = 0;
x=0;
y=0;
l=0;
m=0;

%for loop used for detecting black and white points in the picture.
For a = 1:1:256
   For b = 1:1:256
      If (edge_det_pic1 (a, b) ==1)
         white_points = white_points+1;
      Else
         black_points = black_points+1;
      End
   End
End

%for loop comparing the white (edge points) in the two pictures
For i = 1:1:256
   For j = 1:1:256
      if(edge_det_pic1(i,j)==1)&&(edge_det_pic2(i,j)==1)
         matched_data = matched_data+1;
         Else
            ;
      End
   End
End

%calculating percentage matching.
total_data = white_points;
total_matched_percentage = (matched_data/total_data)*100;

%outputting the result of the system.
If (total_matched_percentage >= 90)
%can add flexibility at this point by reducing the amount of matching.
```

```
    total_matched_percentage
    OUTPUT_MESSAGE
```

IMAGE BINARIZATION

```
[Filename, pathname] = uigetfile ('*.jpg', 'Select jpg sourse file');
If is equal (filename, 0)
   Disp ('User selected Cancel')
Else
RGB = imread (fullfile (pathname, filename));
BW = im2bw (RGB, 0.6);
Image (BW)
Imshow (BW)
%BW1 = gpuArray (imread ('C: \ACADEMICS\img\MATLAB\images.jpg'));
%figure, imshow (BW1)

%BW2 = bwmorph (BW1,'remove');
%figure, imshow (BW2)

%BW3 = bwmorph (BW1,'skel', INF);
%figure, imshow (BW3)
ab=strcat('MATLAB\',num2str(rand()),'.jpg');
Imwrite (BW, ab);
%imwrite (BW, fullfile (pathname,'Fingerprint.jpg'));
End
```

VERIFICATION

```
[Filename, pathname] = uigetfile ('*.jpg', 'Select jpg sourse file');
If is equal (filename, 0)
   Disp ('User selected Cancel')
Else
I=imread (fullfile (pathname, filename));
av_files = dir ('MATLAB\*.jpg*')
ImgNum=size (av_files, 1);
Message='Hi';
For i=1: imgNum
    Name =fullfile ('MATLAB', av_files (i).name);
    a = imread (fullfile (pathname, filename)); %reading images as array to variable 'a' & 'b'.
    b = imread (name);
    AW=im2bw (a, 0.6);
    BW =im2bw (b, 0.6);
    Try
     If AW==BW
    Message='User is valid';
    Break;
    Else
    Message='User is not valid';
    End;
    Catch exception
       Message='User is not valid';
End
End
Msgbox (message);
End
```