Biometric Security Solutions for Human Authentication

A thesis submitted
in fulfillment of the requirement for the award of degree
of
Doctor of Philosophy

Submitted by

SUNIL KUMAR SINGLA

Supervisor

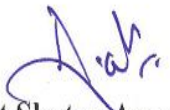
DR. AJAT SHATRU ARORA

Professor, Department of Electrical and Instrumentation Engineering
Sant Longowal Institute of Engineering and Technology, Longowal, Punjab
India

DEPARTMENT OF ELECTRICAL AND INSTRUMENTATION ENGINEERING
THAPAR UNIVERSITY, PATIALA
2011

CERTIFICATE

Certified that the thesis entitled "***Biometric Security Solutions for Human Authentication***" being submitted by **Mr. Sunil Kumar Singla** to the **Department of Electrical and Instrumentation Engineering, Thapar University, Patiala** in fulfillment of the requirements for the award of degree of **"Doctor of Philosophy"** is a record of bonafide research work carried out by him. He has worked under my guidance and supervision and fulfilled the requirements for the submission of this thesis which has reached the requisite standard. The matter presented in this thesis has not been submitted in part or full for the award of any degree in any other University or Institute.



(Dr. Ajat Shatru Arora)

Professor,

Department of Electrical and Instrumentation Engineering

Sant Longowal Institute of Engineering and Technology, Longowal,

Punjab, India

ACKNOWLEDGEMENT

The real spirit of achieving a goal is through the way of excellence and austerous discipline. I would have never succeeded in completing my task without the cooperation, encouragement and help provided to me by various personalities.

First of all, I render my gratitude to the ALMIGHTY who bestowed self-confidence, ability and strength in me to complete this work. Without his grace this would never come to be today's reality.

Although the Knowledge like electricity pervades everywhere yet the Teacher is the point where it shines as light. I am extremely lucky to have an opportunity to blossom under the supervision and guidance of **Dr. Ajat Shatru Arora**, Professor, Sant Longowal Institute of Engineering and Technology, Longowal who helped me to grow like Phoenix out of the ashes of my shortcomings and failures. His charismatic personality delves in knowledge to bring zeal and enlightenment in the lives of not only his students but also the humanity. To me, he is not mere a man but a current of love who treaded with me through thick and thin.

Dr. A. Mukherjee, Director, Thapar University, Patiala, Dr. K. K. Raina, Deputy Director, Thapar University, Patiala, Dr. P. K. Bajpai, Dean, Research and Sponsored Projects, Thapar University, Patiala, Prof. S. Ghosh, Head of Department, Electrical and Instrumentation Engineering and my colleagues supported me in this Endeavour to the best of their abilities. I am modestly bowing my head in the feet of divine Lord to thank them all for their love, support and blessings.

I am thankful to my doctoral Committee members Dr. R. K. Sharma, Professor, Thapar University, Patiala and Dr. Sanjay Jain, Associate Professor, Thapar University, Patiala for their help, valuable suggestions and constant encouragement through out the period of research.

A boat held to its moorings will see the floods pass by; but detached of its moorings, may not survive the flood. The support of all the members of family enthused me to work even while facing the Blues. I take pride of myself in being the son of ideal parents who sacrificed their little joys to bring me to the realization of my dreams and their hopes. It is said that realization comes to those who are immersed in love. It is undoubtedly a rare bliss to be a son of compassionate and affectionate parents who priorities you above everything in their lives. Lady luck has graced me with loving wife, Shaily, who is always a source of encouragement and inspiration. My

brother, Ravinder, always acted as a catalyst to show me the correct path through out my life. I thank him for his love, support and devotion towards me. I am also thankful to my Bhabi Alka, Little Kritika and Gunjan for their concern towards my work. I am thankful to my father in law, my mother in law, my brother in law and sister in law for their blessings and motivation.

I owe something more to my son, **Sahil**, from whom I borrowed several weekends and evenings for completion of this pursuit. I am also thankful to my friends Dr. Kulbir Singh, Mr. Ajay Kakkar, Mr. Gurvinder Singh, Mr. Gaurav Mittal and Mr. S. P. Yadav for their help and motivation.

Finally, I would like to thank all the persons who directly or indirectly helped me for the completion of this work.

Sunil Kumar Singla

Dedicated to

the dreams of my parents....

ABSTRACT

In the present day of automated world, machines are replacing the human in every aspect of life. Due to this, the security concern regarding the authenticity of the user goes on increasing. Hence, it becomes necessary to include some constrains in order to reject imposters (unauthorized persons) and allow only the authorized user to access automated services. Biometric can provide the solution to these problems. Although a lot of work has been done in the field of biometric, particularly, in the field of fingerprint biometric, nevertheless objective of highly secure practical solution is still to be achieved. Present thesis is an attempt to propose biometric based security solutions for human authentication with improvement in existing techniques and solutions based on level of security concerns. In the initial part the major problems in minutiae based fingerprint authentication system have been addressed. The improved algorithms for thinning, minutiae extraction and relative alignments of query and reference fingerprint images have been proposed. In addition to that an image based fingerprint verification system; a combination of biometric (voice) with conventional method (password) and a fuzzy logic based multibiometric system using fingerprint and palmprint has also been proposed.

An improved thinning algorithm (preprocessing step in minutiae based system) has been proposed and implemented by using the Karnaugh map (K-Map) technique in which all the rules are simultaneously applied to each and every pixel which resulted in faster response as compared to look up table technique. The response time of the system has further been reduced by improving the window extraction time and by using the short circuit logical operators. Single isolated pixels are also removed from thinned image as they are not required in the final minutiae extraction stage. Rotation independent thinned skeleton of one pixel width and overall significant reduction of CPU time has been achieved with the proposed method.

Crossing Number method is one of the most widely used binarization based method for minutiae extraction but is highly depends upon the pre-processing steps and is not robust against the spikes (a non minutiae point which is required to be eliminated in the post processing step). A new method has been proposed for the minutiae (feature) extraction. In the proposed method only the genuine cases of minutiae have been identified and solved to a minimized logical

expression using a well known minimization technique of Karnaugh map. The capability of the proposed algorithm has further been enhanced by including the steps to remove the boundary pixels. The proposed method eliminates up to 25% false minutiae in the extraction stage, which remains with the crossing number method.

In order to find the rotation and/or translation between the reference image and query image a Genetic Algorithm (GA) based relative alignment algorithm has been proposed. In the proposed algorithm there is no need to find the reference core or delta point because reliable detection of these reference points is a difficult task. In the proposed algorithm, all the three parameters x, y (translation) and θ (rotational) have been optimized separately. The processing time of the GA based algorithm has been improved by considering the range of deviation of the query data point from the reference data point and by using the binary search algorithm.

An image based fingerprint verification system using LabVIEW (Laboratory Virtual Instrument Engineering Workbench) has been implemented. The proposed method uses a learning phase, which is not present in conventional image-based systems. The rotation and translation between the query and reference image has been taken care by calculating and comparing the circular intensity profile of both the images. Further in order to increase the speed of the system, sub sampling of the image has been performed which reduces the amount of data required for matching. The size of the template is very critical for the success of image based system. The simulation results had been obtained for three different sizes of template images (i.e. 50×50, 100×100 and 200×200) and for different thresholds (threshold of 700, 750, 800, 850 and 900). For the smaller size template image (50×50) the false rejection rate is less in comparison to larger learning images but false acceptance is high. So, a compromise has to be made between false acceptance and false rejection. Simulation results for different fingerprints with various learning image sizes of FVC2002/Db1_a database reveal that a 100×100 learning image size for a threshold value of 700 (1000 being the perfect match) gives good results for false acceptance rate (FRR) and false rejection rate (FAR). A FRR of 1.027% and FAR of 0% have been achieved with 100×100 sized template image at a threshold of 700. Further, the fingerprint images have been enhanced using the STFT analysis and contextual filtering in the Fourier domain and processed in the similar way to find false acceptance and false rejection rates. On comparing the enhanced database results with the original database results it has been observed that the later (original) are better than the former (enhanced). This is due to the fact that

although with enhancement ridge- valleys structure of the fingerprint improves but much richer grey-level information of a fingerprint image has been lost.

Finally, in order to overcome limitations of single biometric such as non uniqueness, noise and intra class variation etc., two solutions have been proposed. In the first solution, a system integrating a single biometric (speech) with conventional method (password) has been developed. In the developed system, the first stage identifies the group of persons on the basis of biometric (speaker identification) and second stage authenticates the person on the basis of password from the list of selected entries in the first stage. The proposed integrated system has increased the accuracy of the system to 99.875% (with ten entries extracted in the first stage) and at the same time also overcomes the problem of non-enrollment of the user. In the second solution, two biometric traits, palm print and fingerprint have been combined at the score level using Fuzzy logic based system. Three different sets of if-else rule have been formulated for low, medium and high security. In order to overcome the problem of non universality the rules for the low security system, have been formulated in such a way that if any of the inputs is with a reasonable score then the system accepts the claim of the user. With this type of arrangement 0% false rejection rate and 0.75% false acceptance rate has been achieved. With the formulated rules of medium and high security false rejection rate increased to 1.61% and 2.88% respectively from the 0% for low security but false acceptance rate get reduced to 0.225% and 0% respectively.

Further, a two step very high security system has also been proposed in which another biometric trait (voice) has been added with the palm and fingerprint to enhance the security. The three biometric traits have been combined in such a manner that the voice biometric identifies the person while the combination of palm and fingerprint authenticates the person. Findings of this research work can be utilized to improve existing human authentication systems.

TABLE OF CONTENTS

List of Figures

List of Tables

CHAPTER 1

Introduction

1.1 Preamble

The word biometric comes from the Greek words bio and metric, meaning ``life measurement" [1]. Generally speaking, biometric is the study of measurable biological characteristics or personal trait [1, 2]. In lay-man's terms, a physical characteristic can be defined as things *that we are,* while a personal trait can be defined as things *that we do*. Examples of physical characteristics are:

- Fingerprints
- Eye features such as iris or retina
- Facial features
- Hand geometry
- Palmprint

Examples of personal traits are:

- Handwritten signatures
- keystrokes or typing
- voice print

"Biometric" is a general term used alternatively to describe a characteristic or a process, where as a characteristic, it is a measurable biological (anatomical and physiological) & behavioral characteristic [3] that can be used for automated recognition and as a process it is an automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics [4].

This technology is becoming popular on pretext that each person has specific unique physical characteristics that can't be lost, borrowed or stolen. In the present day of automated world, machines are replacing the human in every aspect of life. Due to this, the security concern regarding the authenticity of the user goes on increasing. Hence, it becomes necessary to include some constrains in order to reject imposters (unauthorized persons) and allow only the authorized user to access automated services.

In practice there are two traditional methods to check identity of a person [1, 2], these are:

- **Ownership**: Something you have (Key, Smart cards, etc.), also known as token based approach
- **Knowledge**: Something you know (PIN, Password etc.)

These traditional methods of checking someone's identity actually suffers from a common problem of inability to differentiate between an authorized person and an imposter who fraudulently acquires the access privilege of the authorized person [2, 5]**,** for example**,** in the knowledge-based approach, to some extent, the "knowledge" can be guessed, forgotten or shared and in the token-based approach, the "token" can be easily stolen or lost. These weaknesses generate serious financial damage to companies and societies. The following are some interesting statistics:

- ❖ According to Javelin Strategy and Research (2009) [6], in 2008, existing account fraud in the U.S. totaled **$31 billion.**
- ❖ Almost 10 million Americans learned they were victims of identity fraud in 2008, up from 8.1 million victims in 2007 [7].
- ❖ According to Aberdeen group, businesses across the world lose **$221 billion** a year due to identity theft [6].

The search is on for better ways of proving identity. As computer power has grown, it leads to an idea that the automated capture, measurement and identification of distinctive physiological or behavioral characteristics could safeguard our identities and provide security to our property, privacy etc.. The technologies now being developed for these purposes have come to be labeled 'biometrics'. Biometric is a technology that relies on **"Something that you are** or **something you do".**

1.2 History of Biometric

Measurement of physical features such as height, eye color etc., as a method of personal identity is known to date back to the ancient Egyptians. Archaeological evidence of fingerprints being used to associate a person with some event or transaction is also said to date back to ancient China, Babylonia and Assyria. But it was not until the end of the 19th century that the study of biometrics entered the realm of crime detection. Alphonse Bertillon, a French police clerk and anthropologist, pioneered a method of recording multiple

body (anthropometric) measurements, physical descriptions and photographs for individual identification purpose. It was adopted by many police authorities worldwide during the 1890s, but soon became obsolete once it was recognized that people could indeed share the same physical measurements [8, 9]. Meanwhile, the quest for a physical identifier that was unique to each individual gained significant ground when British anthropologist, Sir Francis Galton, worked on the principle that fingerprints were permanent throughout life, and that no two people had identical fingerprints [10]. Galton calculated the odds of prints from two people being identical to be 1 in 64 billion and also identified characteristics – known as 'minutiae' – that are still used today to demonstrate that two impressions made by the same finger match. Galton classified the fingerprints as whorl, arch and loop [8, 11].

In 1897, Sir Edward Henry and colleagues established a modified classification system based on Galton's observations, allowing fingerprints captured on paper forms using an ink pad to be classified, filed and referenced for comparison against thousands of others. By 1901, Henry's fingerprinting system had been adopted in the UK by Scotland Yard [12] and its use then spread through most of the world to become a standard method of identity detection and verification in criminal investigations. In 1904, fingerprint bureaus were established in United States at Leavenworth, Kansas and the St. Louis, Missouri. In 1921, the "Identification Division of the FBI" was set up [13]. In 1936, Ophthalmologist Frank Burch proposed the concept of using iris patterns as a method to recognize an individual [14]. The first semi-automatic face recognition system was developed by W. W. Bledsoe in 1960. This system locate the facial features such as eyes, ears, nose and mouth on the photographs and calculates distances and ratios to a common reference point that was compared to the reference data [15]. A Swedish Professor, Gunnar Fant, 1960, published a model based on the analysis of X-rays of individuals describing the physiological components of acoustic speech production and in 1970, Dr. Joseph Perkell extended this model by including the tongue and jaw. The model provided a more detailed understanding of the complex behavioral and biological components of speech [16]. The first commercial hand geometry recognition systems became available in 1974 for applications in physical access control, time & attendance and personal identification. In 1977, a patent was awarded for the personal identification apparatus that was able to acquire dynamic pressure information [16]. In 1985, David Sidlauskas awarded the patent of hand geometry for identification. In 1987, Sirovich

et al. [17] applied principle component analysis technique to the face recognition problem. This was a milestone because it showed that less than one hundred values were required to approximate a suitably aligned and normalized face image. In 1994, Dr. John Daugman was awarded a patent for his iris recognition algorithms. The FBI launched Combined DNA Index System (CODIS) to digitally store, search and retrieve DNA markers for forensic law enforcement purposes in 1998. In 2001, Lm et al. [18] published the first research paper for biometric recognition by using hand vein pattern. The International Standardization Organization (ISO) established the ISO/IEC JTC1 Subcommittee 37 (JTC1/SC37) to support the standardization of generic biometric technologies in 2002 [16]. The Subcommittee develops standards to promote interoperability and data interchange between applications and systems. In 2003, the European Biometric forum was established. In 2004, Connecticut, Rhode Island and California established statewide palm print databases that allow law enforcement agencies in each state to submit unidentified latent palm prints to be searched against each other's database of known offenders [19]. In order to give boost to biometric, in 2005, NIST along with national security agency of USA have sponsored a number of biometric-related activities including the development of a common biometric exchange file format (CBEFF) , NIST biometric interoperability, performance and assurance working group etc. [20]. In 2006, the department of passport USA (United States of America) began to issue biometric passports to diplomats and other officials. Later in 2006, biometric passports were issued to the public. Since august 2007, the department has issued only biometric passports [21]. In 2009, Indian government has set up National Authority for Unique Identity to provide multipurpose national identity card to each of its 1.25 billion people, carrying the biometric information of the individual. The project is expected to be completed in 2011 [22].

1.3 Properties for a Good Biometric

Theoretically psychological or behavioral characteristics of human being can be used to make personal identifications only if it has following properties [23, 24]:

- **Universality,** which means that every person, should have the required characteristic which can be used as a biometric.

- **Uniqueness,** which means that any characteristic to be used as a biometric, possessed by two different persons must be distinctive enough.
- **Permanence** means that the characteristics must be invariant with time, position and conditions.
- **Collectability** means that the required characteristic must be easily measureable.

Practically following parameters are also required

- **Performance** means that a system needs to perform quickly and accurately.
- **Acceptability** means that the people must accept the system easily.
- **Circumvention** refers to how easy it is to fool the system by fraudulent techniques?

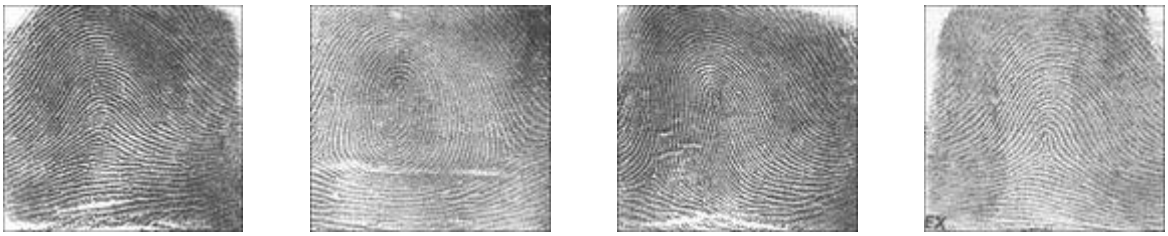
1.4 Biometric Modalities

The most common biometric modalities include fingerprint, face, iris, voice, hand geometry, palm print. There is no single biometric modality that is best for all implementations. Each modality has its advantages and disadvantages. Many factors must be taken into account when implementing a biometric system including location, security risks, task (identification or verification), expected number of users etc. In this section, a brief introduction of different biometric modalities is presented.

1.4.1 Fingerprint

Fingerprint biometric is the most commonly used biometric technique [25-28]. Since the late nineteenth century, fingerprint identification methods have been used by police agencies around the world to identify both suspected criminals as well as the victims of crime. A fingerprint is a smoothly flowing pattern of alternating valleys and ridges [29,30], the ridges and valleys being parallel in most regions. Several permanent and semi-permanent features such as scars, cuts, bruises and cracks are also present in a fingerprint. The patterns and geometry of fingerprints are different for each individual and they are unchanged as body grows [1]. The fingerprint patterns are hereditary. They are formed before the birth, while one is still in the womb, they never change throughout the lifetime and they are even around for a while after one dies. They are totally unique, Even identical twins sharing the same DNA also have different fingerprints. The classification of fingerprints is based on certain

characteristics as whorl, right loop, left loop, arch, twin loop, and tented arch as shown in Figure 1.1.



Arch | Loop (Right Loop) | Whorl | Arch (Tented Arch)

Figure 1.1 Classification of fingerprints

Because of their uniqueness and consistency over time, rich feature information fingerprints have been used for authentication for many years, more recently becoming automated (i.e. a biometric) due to advancements in computing capabilities. Fingerprint authentication systems are secure, fast, reliable and easy to use. The other advantage of fingerprint recognition is that fingerprint scanners are small, which can be embedded in laptops, mobile phones and personal digital assistants. But a small portion of the population cannot provide clear fingerprint images due to aging and genetic problems; moreover, their use for access security requires special input devices [5].

1.4.2 Voice

Voice is a combination of physiological and behavioral biometric. The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound [5]. These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions such as common cold, emotional state, etc [23].

The automatic recognition process of the human voice is often divided in speech recognition and speaker recognition [31]. These two areas use the same input signal (the voice), but not for the same purpose, the speech recognition aims to recognize the message uttered by any speaker, and the speaker recognition wants to identify the person who is

talking. This method captures the sound of the speaker's voice as well as the linguistic behaviors. The speaker-specific characteristics of speech are due to differences in physiological and behavioral aspects of the speech production system in humans [32]. These systems rely on very low-cost devices (hardware requirement is very low), they are generally the least expensive systems to implement for large numbers of users and the acceptability level is very high in this type of biometric system. It would allow a remote verification using the phone such as phone banking but, these systems suffers from drawbacks like mimicry by imposter or recording the voice of the authorized person or emotional statement of the authorized person [5].

1.4.3 Hand Geometry

Hand geometry recognition systems are widely used for applications in physical access, attendance tracking and personal verification. They have found a sustainable market through use in security and accountability applications. Their ease of use, stand-alone capabilities, and small data requirements make them a popular choice for those in need of authentication systems.

Hand-geometry-based systems require the subject to place his or her hand (usually the right hand) on a plate where it is photographically captured and measured. This method measures certain key features of the hand like length of fingers and thumb, the width between two points, thickness, surface area of an individual's hand etc [32]. The image captures both the top surface of the hand and a side image that is captured using an angled mirror. Hand geometry data is easier to collect . Since the user has to perform an obtrusive task (placing his or her hand on the platen for sampling), because of this obtrusiveness, subjects cannot have their biometric features sampled without their knowledge. So, hand-based biometrics represent less of a privacy threat than some other systems also hand geometry can be easily integrated with other biometrics [32] but, It has the limited accuracy and shape of every person's hand is not necessarily different than another person's hand also the shape of a person's hand changes significantly over a time period .

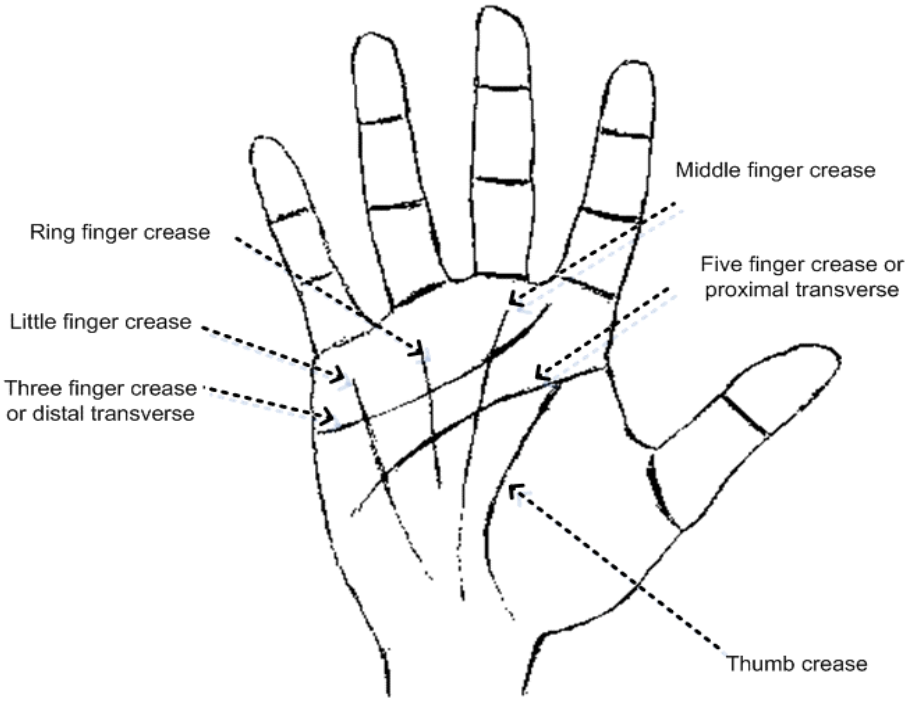


Figure 1.2 Hand geometry

1.4.4 Palm Print

Palmprint, the inner surface of our palm normally contains three flexion creases, secondary creases and ridges. The flexion and secondary creases are also called principal lines and wrinkles respectively. The flexion creases and the main creases are formed between the 3rd and 5th months after conception [33] and superficial lines appear after birth. These creases are not genetically deterministic. Even identical twins who share the same DNA sequences have different palmprint [34].

These non-genetically deterministic and complex patterns have rich information for personal identification. There are two types of palmprint recognition research, high resolution and low resolution approaches. High resolution approach is suitable for forensic applications such as criminal detection, while low resolution is more suitable for civil and commercial applications such as access control.

Figure 1.3 Palmprint(a) High resolution image (b) Low resolution image

The advantage of using palm print is that they cannot be acquired without the knowledge of the person. Moreover, the uniqueness and permanence of palmprint is also high while its universality is medium.

1.4.5 Face

Face is a primary focus of attention in social intercourse, playing a major role in conveying identity and emotion. With the advancements in computing capability over the past few decades, face biometric comes into picture.

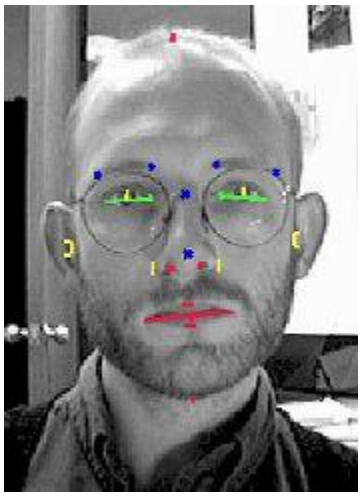


Figure 1.4 Features of face

This type of biometric system use PC-attached cameras to capture the facial geometry [1] and records a number of points and measurements, including the distances between key characteristics such as eyes, nose and mouth, angles of key features such as the jaw and

forehead, and lengths of various portions of the face. Using this information, the program creates a unique template incorporating all the numerical data. This template may then be compared to enormous databases of facial images to identify the subject. Face recognition based biometric system is highly accurate and gives good performance, also this type of biometric system is fast but, because of the camera cost, the system is costly and acceptability of the system is also less [5].

1.4.6 Iris

The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The automated method of iris recognition is relatively new, existing in patent only since 1994. Iris scanning measures the iris pattern in the colored part of the eye (although the color has nothing to do with the scan). The Iris forms during the early stages of fetal development and is complete by the eighth month. It is highly distinctive and will not be same even for the identical twins [5]. The iris pattern of one's left eye is also different from the iris pattern of the right eye. The retinal blood vessels highly characterize an individual, so, accuracy is one of the advantages of this method of identification [31]. Duplicate artificial eyes are useless since they do not respond to light but blind people or people with severe damaged eyes (diabetics) will not be able to use this biometric method. Acceptability is another problem for the iris based biometric system [5]. Moreover the specialized cameras are required which increases the cost and size for this biometric system.

1.4.7 Signature

Signature is a behavioral biometric and is widely accepted in governmental, legal and commercial transactions. The signature biometric systems measures the physical activity of signing, such as the pressure applied, the quantity & directions of the strokes , overall size of the signature, speed etc. [35,36] .

Figure 1.5 Signature biometric

While it is easy to copy the image of a signature, it is extremely difficult to mimic the behavior of signing [35, 37]. People are used to sign documents, so signature recognition systems are not perceived to be invasive. People may not always sign in a consistent manner because many factors can influence the consistency of signatures such as emotional and physical conditions. Furthermore, professional forgers are capable of reproducing signatures to fool recognition systems. In conclusion it can be said that collectivity and acceptability of the signature biometric are high while its performance and permanence are low.

1.4.8 Deoxyribonucleic Acid (DNA)

DNA is a nucleic acid containing all genetic instructions for development of organs, is commonly applied to forensic applications such as criminal investigation and corpse identification. Everyone has unique DNA pattern, except identical twins [38, 39]. DNA can be extracted from blood, hair, skin etc., which can always be collected in crime senses. One of major concerns of using DNA for personal identification is privacy since DNA can be collected unintentionally and contains all genetic information including genetic disorder. The accuracy level of DNA is very high [40]. The universality and permanence of DNA is also high but collectivity and acceptability of DNA as a biometric is low. Moreover, whole DNA process is too costly.

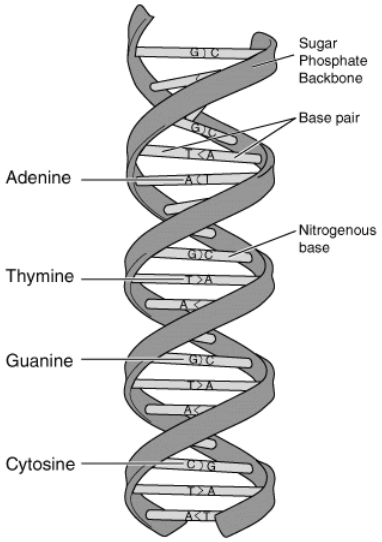


Figure 1.6 DNA biometric

1.4.9 Keystroke Dynamics

Keystroke dynamics is a behavioral measurement and it aims to identify users based on the typing characteristics of the individuals such as duration of a keystroke or key hold time, latency of keystrokes or inter keystroke times, digraph or length of time between consecutive keystrokes, typing error and keystroke pressure [41, 42]. This technology is relatively cheaper than the fingerprint or retinal scan technology, which requires expensive and extra hardware for data collection. Keystroke dynamics do not require any extra hardware [43] but the uniqueness, performance and permanence of this biometric are low.

1.4.10 Hand Vein Recognition

This type of biometrics can be used to identify individuals based on the vein patterns in the human finger. The technology works by identifying the subcutaneous (beneath the skin) vein patterns in an individual's hand. When a user's hand is placed on a scanner, a near-infrared light maps the location of the veins. The red blood cells present in the veins absorb the rays and show up on the map as black lines, whereas the remaining hand structure shows up as white. After the vein template is extracted, it is compared with previously stored patterns and a match is made. The vein patterns are unique to each individual [44, 45]. The vein pattern does not change over time (except from size). This feature makes it suitable for one-to-many matching, for which hand geometry and face recognition may not be suitable. But invasiveness, acceptability and cost are some of the issues that restrict the use of hand vein biometric.

1.5 Choice of the Biometric Trait

There are several biometric techniques in use/ under investigation such as fingerprint, iris, retina, hand geometry, palmprint, hand vein, voice, face, signature, DNA, Keystroke etc.. Each biometric technology has its strengths and limitations. A brief comparison of different biometric traits is given in Table 1.1.

Table 1.1 Comparison of different Biometric modalities [29]

	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Fingerprint	M	H	H	M	H	M	M
Voice	M	L	L	H	L	M	H
Hand Geometry	M	M	M	H	M	M	M
Palmprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Iris	H	H	H	M	H	L	L
Signature	L	L	L	H	L	H	H
DNA	H	H	H	L	H	L	L
Keystroke	L	L	L	M	L	M	M
Hand Vein	M	M	M	M	M	M	L

***M**= Medium, ***H**=High, ***L**=Low

Although each of these biometric techniques, to a certain extent, possesses the above mentioned desirable properties and has been used in practical systems or has the potential to become a valid biometric technique, but no single biometric trait can effectively meet the requirements of all the applications [29, 46]. Moreover, deployability (device size, environmental conditions and infrastructure requirements), invasiveness (the level of involvement required by the user) and implementation cost are the other issues which need to be taken care for the selection of a particular biometric.

The fingerprint trait has a very good balance of all these desirable properties. Fingerprints are unique [47] and they rarely change throughout the life [48]. Even identical twins having similar DNA have different fingerprints [49]. Every person has fingerprints with the exception of very few people. More over acceptability and deployability of fingerprint is very high as size & infrastructure requirements are very less. In Fingerprint biometrics the image of only exterior features is required so they are non invasive. The

implementation cost of fingerprint biometric is also less in comparison to other biometrics (with the exception of voice). Owing to the above reasons the fingerprint has been chosen as the parameter for the further investigation.

From the literature review it has been found that there is still a scope to work in the following areas for the fingerprint verification:

1. Inaccurate alignment i.e translation and rotation of the test image and the reference image.
2. Preprocessing/enhancement of the poor quality signals.
3. Deletion of the spurious minutiae from the test and reference representation.

A biometric system which relies only on a single biometric identifier in making a personal identification is often not able to meet the desired performance requirements [50]. Noisy data, performance limitation, circumvention and non-universality (leading to failure-to-enroll) all affect the performance, security and convenience of using such a system. Some of the limitations imposed by single biometric systems can be overcome by *multibiometric systems*. These systems take the samples of more than one biological characteristics or personal trait. Multibiometric systems-

(i) Address the problem of non-universality, since multiple traits ensure sufficient population coverage

(ii) Address the problem of non uniqueness caused by single biometric which may increase the false accept rate

(iii) Address the problems of noise and intra class variation present in single biometric which results in false reject rate (FRR)

(iv) Provide anti-spoofing measures by making it difficult for an intruder to “steal” multiple biometric traits of a genuine user.

So, multibiometric systems are more reliable and provides higher security and verification rates due to the presence of multiple, independent pieces of evidence. For this purpose of developing multibiometric system (using different biometric traits) voice and palm print along with fingerprint have been chosen as other biometric traits because voice biometric is natural, user find it noninvasive. Moreover, acceptability and deployability of voice is very high. Palm print biometric has a high uniqueness and medium acceptability

and circumvention. The palm print of a person cannot be acquired without the knowledge of the person which is very critical aspect in high security applications. Also the implementation cost of palm print biometric system is less than that of face or iris biometric because of the low cost of scanner compared to high resolution cameras.

1.6 Objectives of the Thesis

The objectives of the Ph.D research proposal titled **"*Biometric Security Solutions For Human Authentication*"** is to develop algorithms for the human authentication using fingerprint with a view of

(i) Image preprocessing/enhancement for low quality signals

(ii) Inaccurate alignment

(a) Translation

(b) Rotational

and/or thereof using soft / evolutionary computational techniques.

(iii) Testing the developed algorithm with the standard database/ recorded in the lab

(iv) To explore the possibility of combining the fingerprint biometric with other biometric parameter for enhancing the security of the system.

1.7 Contributions in the Thesis

Based upon the literature survey and keeping in mind the objectives of the thesis in the present work, improved algorithms for thinning, minutiae extraction and relative alignments of query and reference fingerprint images have been proposed. In addition to that an image based fingerprint verification system; a fuzzy logic based multibiometric system using fingerprint and palmprint, a combination of biometric (voice) with conventional method (password) has also been proposed. The brief description of the contribution in the thesis is as follows

1. Thinning is an important pre-processing step in minutiae based automatic fingerprint identification systems, as a good thinned image map can facilitate the minutiae extraction. An improved thinning algorithm has been developed which provides the thinned fingerprint skeleton of one pixel width and also makes the thinning rotation independent. In the proposed algorithm single isolated pixels are removed as they are

not required in the final minutiae extraction stage and by using the Karnaugh map technique all the rules are simultaneously applied to each and every pixel which resulted in faster response as compared to look up table technique. The response time has further been reduced by improving the window extraction for templates and by using the short circuit logical operators. An improved thinned image and overall significant reduction of CPU time has been achieved with the proposed methods.

2. Feature extraction is a very important step in a human authentication system. The minutiae based identification systems have been popular because of their accuracy and less complexity. Crossing Number method is one of the most widely used binarization based method for minutiae extraction but, is not robust against the spikes and tends to register spike as minutiae, also the method highly depends upon the pre-processing steps such as thinning. A new method has been proposed for the minutiae extraction which uses genuine cases only. All these cases are solved to a minimized logical expression using a well known minimization technique of Karnaugh map. The proposed method eliminates up to 10% false minutiae in the extraction stage, which remains with the crossing number method. The capability of the proposed algorithm has further been enhanced by including the steps so that the boundary pixels should not be included in the list of minutiae.

3. Rotation and translation between the reference image and query image are the major issues involved for the success of an automatic fingerprint authentication system. Because, rotation and translation between the two images make it difficult to find the correspondence between the features (minutiae) of the two images. A Genetic Algorithm (GA) based relative alignment algorithm for the alignment of reference and query fingerprint image has been proposed. In the proposed algorithm there is no need to find the reference core or delta point because reliable detection of these reference points is a difficult task. In the proposed algorithm, all the three parameters x, y (translation) and θ (rotational) have been optimized separately. In order to improve the processing time, two steps, one of which uses binary search algorithm and other uses the range of deviation of the data from the query image, have been implemented.

4. A new image based fingerprint verification system using LabVIEW (Laboratory Virtual Instrument Engineering Workbench) toolbox version 6i has been proposed and implemented. The proposed method uses a learning phase, which is not present in conventional image-based systems. The rotation and translation between the query and reference image has been taken care by calculating and comparing the circular intensity profile of both the images. Because the circular intensity profile of the translated image will be same while for the rotated image it will be same but shifted to right or left depending upon the amount and direction of rotation. Further, in order to increase the speed of the system, sub sampling of the image has been performed which reduces the amount of data required for matching.
5. In order to decrease the false reject rate and to overcome some of the limitations such as non uniqueness, noise and intra class variation imposed by single biometric a combination of biometric and tradition method (password) for speaker identification has been proposed. The proposed method not only solves the above problems of single biometric but also overcome the problem of non enrollment of the user in the system. The improved results have been obtained by the proposed method than the single biometric method. The proposed model can be implemented using any of the other biometric traits.
6. A new fuzzy logic based technique to fuse the multi biometric traits at the score level has been proposed for the high, medium and low security using the fingerprint and palmprint. In low security system in order to take care the problem non universality the rules are framed in such a manner that the matching of only one biometric is sufficient. In high security system the rules have been proposed to overcome the problem of false acceptance. While, the medium security system is the tradeoff between false acceptance rate and false rejection rate. Further, a two step very high security system has also been proposed in which another biometric trait (voice) has been added with the palm and fingerprint to enhance the security. The three biometric traits have been combined in such a manner that the voice biometric identifies the person while the combination of palm and fingerprint authenticates the person.

In the subsequent chapters a detailed description including methodology, experimentation and results of each of these contributions has been provided.

CHAPTER 2

Literature Survey

To achieve the objectives laid out for the present work, extensive literature survey was done to decide the direction of work. The present chapter puts forth the pioneer work done in the field of fingerprint as biometric and multibiometric including fingerprints. In this chapter image and minutiae based fingerprint authentication systems have been discussed. The multimodal biometric techniques have also been discussed with reference to the fusion at the different stages and their relative merits and demerits.

2.1 Background

Archaeological evidence has shown the interest in fingerprints and their use by ancient civilizations. In Nova Scotia a picture writing of a hand with ridge patterns was discovered while fingerprint impressions were found on a standing stone on Goat Island. In ancient China, thumb prints were found on clay seals [51]. However, first scientific paper on fingerprints was published in 1684 by Dr. Nehemiah Grew, describing his systematic study of ridges, furrow and pore structure in fingerprints. In 1686, Professor Marcello Malpighi, at the University of Bologna, noted ridges, spirals and loops in fingerprints. Since then, many persons carried out the study on fingerprints. In 1788, Mayer made a study on the anatomical formation of fingerprints and identified many ridge characteristics [52]. Professor John Evangelist Purkinje, in 1823, published his thesis entitled "A Commentary on the Physiological Examination of the Organs of Vision and the Cutaneous System" in which he identified 9 fingerprint patterns of fingerprints [53]. In 1858, Sir William James Herschel, Chief Magistrate of the Hooghly district in Jungipoor, India, first used fingerprints on native contracts [54]. He used the prints of the right index and middle fingers--on every contract made with the locals. Personal contact with the document, they believed, made the contract more binding than if they simply signed it. As his fingerprint collection grew Herschel began to note that the inked impressions could, indeed, prove or disprove identity. Dr. Henry

Faulds, in 1880, published an article in the scientific journal, "Nature" discussing the use of fingerprints as a means of personal identification and advocated the use of printers ink, as a method for obtaining such fingerprints [55]. In 1882, Gilbert Thompson of the U.S. Geological Survey in Mexico used his own thumb print on a document to prevent forgery. In 1892, Sir Francis Galton published his book, "Fingerprints", establishing the individuality and permanence of fingerprints i.e. no two fingerprints are exactly the same and fingerprints do not change over the course of an individual's lifetime. According to his calculations, the odds of two individual fingerprints being the same were 1 in 64 billion. He classified the fingerprints as arch, loop & whorl and also identified the characteristics by which fingerprints can be authenticated [56]. In 1899, Sir E. R. Henry established the Henry system of fingerprint classification. He further classified the arch, loop & whorl (Galton work) into tented arch, arch, right loop, left loop and Whorl [57]. The fingerprint branch at New Scotland Yard (London Metropolitan Police) was created in July 1901 using the Henry system of classification. During the early part of twentieth century the fingerprint recognition was formally accepted as a valid personal identification method [58] and fingerprint characteristics were well understood as:

- Ridges and valleys have different characteristics for different fingerprints
- Fingerprints can be classified because configuration of each fingerprint vary within a limited range
- The structure of fingerprint pattern remain unchanged over the period of time

During the next 25 years more and more law enforcement agencies join in the use of fingerprints as a means of personal identification. In 1924, the FBI fingerprint identification division was set up with a database of 810,000 fingerprint cards. This database goes on increasing and by 1946, the FBI had processed 100 million fingerprint cards in manually maintained files. Because of the large database and increasing processing requests FBI started to develop automatic fingerprint identification system in 1960 [59]. With the introduction and success of live-scan technology the fingerprint authentication system grew rapidly. In 1977, the Royal Canadian Mounted Police began operation of the first automatic fingerprint identification system (AFIS) system. Now a days automatic fingerprint

authentication system has been used by many countries and in many fields such as access control, financial (tele-banking), medical, forensic applications etc..

2.2 Fingerprint Features

Fingerprints consist of raised friction ridges of skin separated by recessed valleys of skin. A fingerprint is characterized by the curved formation of ridges on a finger. Fingerprints are identified by both macro and micro features [5].

Some of the macro features of the fingerprint are

- Ridge pattern
- Ridge pattern area
- Core Point
- Delta point
- Ridge count

Some of the micro features of the fingerprint include

- Ridge ending
- Ridge bifurcation
- Enclosure or lake
- Short ridge
- Dot or island
- Crossover etc.

Among the micro features ridge ending and ridge bifurcation are mostly used for authentication.

2.3 Fingerprint Authentication Systems

Broadly, the automatic fingerprint authentication systems can be classified into two categories.

i) Pattern (Image) based systems
ii) Minutiae based systems

2.3.1 Image Based Fingerprint Authentication System

In image based fingerprint authentication system the fingerprint image itself is used as a template or reference image and the intensity values at each and every point of this

template are compared with the intensity values of the query image. Depending upon the correlation between the intensity values of the two images the authenticity of the person can be determined. The correlation between reference image R and query image Q , is [60]

For 0, 1, 2,……., M-1 and = 0, 1, 2,……., N-1

The summation is taken over the image region where reference and query image overlap. The Cross correlation of the system is a measure of similarity between the two images. Higher the value of cross correlation between the two images higher is the similarity between the overlapping portion of the two images and vice versa. Hence, the authenticity of the person can be determined by calculating the cross correlation between the reference and query images.

Due to translation (both in x and y direction) and rotation between the two images the determination of cross correlation directly will not give the valid result. So, either some technique has to be applied which will determine the translation and rotation between the two images before applying the cross correlation or one of the images has to be shifted in the given range of translation & rotation and cross correlation between the two images at each shift has to be determined and the maximum correlation among the group should be taken as the similarity between the two images. For example, If δx, δy and $\delta\theta$ represents the range of probable translation in x, y- direction and rotation respectively, then similarity between the two images is given by

(2.2)

The direct application of the above equation is computationally very expensive. For example, If x and y both are sampled with a one pixel step in the range of $\delta x = \delta y = [-50,+ 50]$ and θ with a step size of 1° in the range of $[-20^{o}, +20^{o}]$ then the direct computation of above equation requires 101 101× 41 cross correlations and each correlation for a size of 400 × 400 pixel size images requires 1,60,000 multiplications and additions. Moreover, skin conditions, finger pressure etc. may cause brightness, contrast, ridge thickness etc. to vary significantly across the different impressions of the same finger. Also, nonlinear elastic distortions may cause the different impressions of the same fingerprint to be different.

In the literature different authors proposed the different solutions to the problems of image based fingerprint authentication systems.

Bazen et al. [61] proposed a three step correlation based fingerprint verification system. In the first step small size templates have been selected in the primary reference fingerprint. In the second step template matching has been used to find the position in the secondary (query) fingerprint image at which the template match the best. Finally, the third step aims to compare the template position in both the fingerprints to make the decision regarding the authenticity. Since in this method small templates have been used which means the correlation has been computed locally i.e for the local position, which is much more stable than the global correlation. So, this method can tolerate the non uniform local shape distortions in the fingerprint, but this method is computationally more expensive and is not capable to deal with rotations of more than 10 degree.

Nandkumar et al. [62] proposed a local correlation based fingerprint matching algorithm. In the proposed algorithm the author used a window size of 42 × 42 pixels around the minutia locations in the template image and 32 × 32 pixels size windows around the corresponding location in the query image. The normalized cross-correlation between the query window and template window is computed and peak is detected. If the peak lie outside 10 pixels from the centre, the correlation between template and query window is zero otherwise this is the absolute value of correlation between the query and template window. The local correlation of all template windows with the corresponding regions in the query image are computed and mean correlation value is found. In this way all the possible correspondence from the alignment stage are tested and maximum correlation value over all the correspondence is taken as the matching score between the query and template image. In the proposed method, minutiae points are required to be extracted so all the problems related to minutiae extraction remains with this system. Moreover, the proposed system depends upon the alignment algorithm used before matching and system is computationally expensive.

Cavusoglu et al. [63] proposed a robust correlation based fingerprint matching algorithm. The proposed algorithm requires segmentation, ridge orientation, reference point detection and normalized operations before the application of correlation algorithm. During the enrollment stage starting from the selected reference (core) point of the template image a

set of features is obtained with different radius (r) and angle θ. For the authentication purpose the features of the input query image are obtained by rotating the query image with an incremental size of 1º in the given range of -15º to + 15º. For each rotation the normalized cross correlation values of both images are calculated. The maximum value of cross correlation in the given range, determine the similarity of the query and template image. This method is efficient in terms of storage since instead of template (reference image or part of reference image) the features of the template are stored but this method requires the accurate detection of core point which is a trivial task. Moreover, this method also fails in case the core point is not present in the fingerprint image.

Owang et al. [64] proposed a correlation based matching method using local Fourier-Mellin descriptor (FMD) and phase only correlation (POC) function. In the proposed method most likely FMD pair is calculated from the reference and query fingerprint images. According to the information obtained from the pair two fingerprints are aligned and other corresponding FMD pairs are checked if they are matched or not. The symmetric phase only correlation function (which is shift and brightness invariant and is robust against noise) is used during the calculation of similarity of the two FMDs and the alignment parameters. The proposed method does not require any minutiae or core information while taking rotation into account. The proposed system is fast but requires efficient method for the extraction of local FMDs to improve the performance of the system.

Ito et al. [65] proposed a band limited phase only correlation (BLPOC) based image matching algorithm. BLPOC method is more robust to the noise and provides a sharper peak to distinguish between the genuine and imposter matching than POC. In the proposed algorithm the translational displacement is obtained using the positions of the core points (if present) in both query and reference images. The rotational alignment is determined by evaluating the similarity between the rotated replicas of the reference image (in the range of -40º to +40º) and the query image using BLPOC function. If either reference or query image do not have the core point then firstly rotational displacement is determined using the above said method and translational displacement between the rotational-normalized image & query image is obtained using the POC function. In the next step, the common effective image area of the same size is extracted from the two images for matching using BLPOC function. The proposed technique is particularly effective for verifying low quality images that cannot be

identified accurately but the detection of the core point and larger number of computations involved for rotation restricts the use of this method. Moreover, the presence of elastic deformations in the image further degrades the system performance.

Zhang et al. [66] proposed another correlation based fingerprint matching method using both Fourier-Mellin transform and band limited phase only correlation. In the proposed algorithm FMT is used to determine the rotational angle between the reference and query images. The proposed system calculates three different angles (depending upon the local maximum values) instead of one in the FMT algorithm and then selects the most appropriate angle using the following verifying steps

(i) Extend the two aligned images

(ii) Compute the correlation of two extended images using POC and maximum of the correlation

(iii) Compute the position of maximum

(iv) If the position is near the origin, two images are well aligned. Otherwise alignment is false and repeat step (i) to (iv) for other two angles.

If none of the three angles will give the satisfactory response then maximum one of the three correlation values will be used to determine the alignment. In the matching step the BLPOC is used to find the correlation between the two images.

The proposed method combines the advantages of BLPOC (sharpness of correlation peak and robustness) and FMT (Rotation and translation) but the performance of the system degrades if the query and reference image contains much noise and that too of different types.

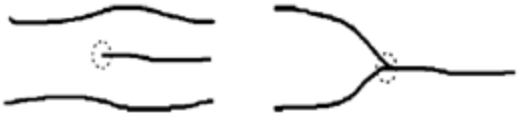
2.3.2 Minutiae Based Fingerprint Authentication System

Minutiae based fingerprint authentication systems are widely used by both human experts and machines. These systems usually rely on "local discontinuities in the ridge flow pattern" called minutiae. According to the empirical study, two individuals will not have more than seven common minutiae [1, 67]. The set of minutiae are restricted into two types:

- Ridge endings
- Ridge bifurcations

Ridge endings are the points where the ridge curve terminates, and ridge bifurcations are the points where a ridge splits from a single path to two paths at a Y-junction as shown in Figure

2.1. The positions and angular orientations of these points within a fingerprint uniquely characterize the fingerprint.



(a) (b)

Figure 2.1 Minutiae points (a) Ridge ending (b) Ridge bifurcation

Broadly, minutiae based verification/identification system is divided into following three steps to find the out the authenticity of the person:

1. Preprocessing of the image
2. Extracting the required information (minutiae extraction)
3. Fingerprint Matching

2.3.2.1 Preprocessing

Preprocessing becomes an essential component of automatic fingerprint identification/verification systems. This step is used to remove that part of the fingerprint image which contains no information and is not required for minutiae extraction. In other words preprocessing of the captured image is performed to enhance the quality of image by removing the useless information. The various steps of preprocessing required in minutiae based system depends upon the manner in which the features (minutiae) are extracted from the fingerprint image. Minutiae extraction methods (discussed in the next section) can be classified into binarization based methods and direct gray scale extraction methods. The binarization based methods require enhancement (if images are of poor quality), segmentation, binarization and thinning as preprocessing steps while direct gray scale extraction methods require enhancement and segmentation as preprocessing steps.

2.3.2.1.1 Image Enhancement

The success of the fingerprint authentication system depends entirely on the quality of the reference and the query image. The clarity of the ridge valley structure defines the quality of the fingerprint image. A good quality fingerprint image has high contrast and well defined

ridges and valleys while a bad quality fingerprints has low contrast and undefined ridges and valleys. Ideally, in a fingerprint image ridge and valley must alternate and flow in a constant direction, so that ridges & valleys can be easily and precisely detected. However, practically due to sensor noise, incorrect finger pressure, skin conditions (e.g. wet or dry, cut or bruises) etc. fingerprints may be of poor quality. The poor quality fingerprint images may lead to false feature extraction which ultimately affects the performance of the system. The goal of an enhancement algorithm must be to improve the ridge valley structure of the fingerprint image so as to enhance the performance of the system. Figure 2.2 represents the good quality, noisy and bad quality fingerprint images.

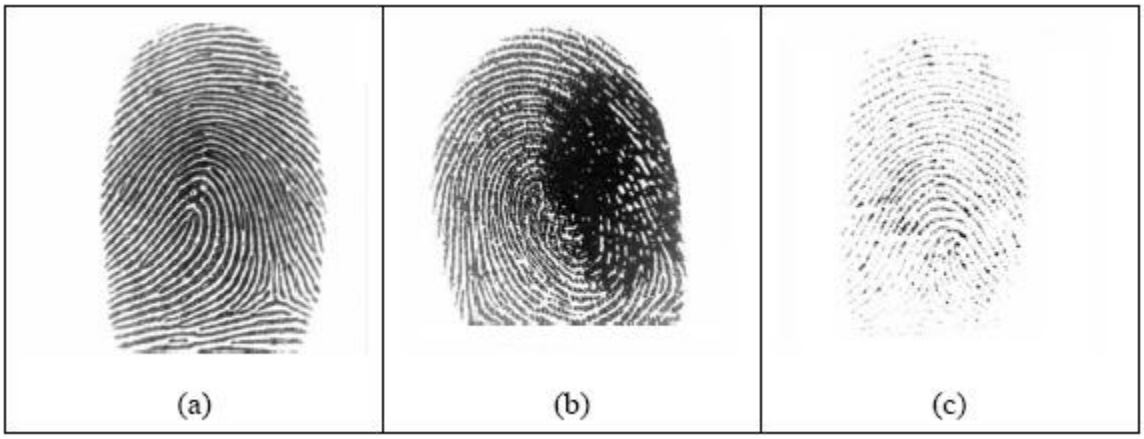


Figure 2.2 Fingerprints of (a) Good quality, (b) Noisy (c) Bad quality

Due to the non-stationary nature of the fingerprint image, using a single filter that operates on the entire image is not effective. Instead, the filter parameters have to be adapted to enhance the local ridge structure. A majority of the existing techniques are based on the use of *contextual* filters. The parameters of contextual filters depend upon the local ridge frequency and orientation.

O' Gorman and Nikerson [68] applied the idea of contextual filtering for the enhancement of fingerprint images. In the proposed method each point of the image is required to be convolved with one of the 16 predefined filters whose orientation best matches with the local ridge orientation. Sherlock and Monro [69] performed contextual filtering in the Fourier domain. The image is convolved with precomputed filters of the same size as that of an image. The precomputed filter bank is oriented in eight different directions at an interval of 45 degree. This algorithm assumes that the ridge frequency is constant through out

the image so, context is determined by the orientation only. Moreover, the algorithm also requires locating the singular points accurately which is a very difficult task in poor quality images.

Hong et al. [70] proposed a fingerprint enhancement method based on the convolution of the image with Gabor filters. The authors used Gabor filters because of their frequency-selective and orientation-selective properties. These properties allow the filter to be tuned to give maximal response to ridges at a specific orientation and frequency. In other words, a properly tuned Gabor filter can enhance the ridges oriented in the direction of the local orientation. For a given frequency ( ) and orientation (φ) the even symmetric two dimensional Gabor filter is given by

– — — (2.3)

Where, and are the standard deviations of the Gaussian envelop along the x and y directions. The choice of and is very critical. With too low value of these parameters the filter will not be robust to noise while too high value may create spurious ridges and valleys. Although, Gabor kernel is beneficial from a time-frequency analysis prospective, it does not necessarily translate to an efficient means for enhancement. Hong et al. assumed that the parallel ridges and valleys exhibit some ideal sinusoidal-shaped plane waves associated with some noises. Unfortunately, their prior sinusoidal plane wave assumption is inaccurate because in some fingerprint images, the signal orthogonal to the local orientation does not consist of an ideal digital sinusoidal plane wave. Yang et al. [71] proposed a modified Gabor filter (MGF) by discarding the inaccurate prior sinusoidal plane wave assumption. The authors have proposed an image independent adaptive parameter selection scheme, which leads to artifacts in some cases. Although, MGF is more accurate in preserving the fingerprint image topography but like GF approach the method fails when image regions are contaminated with heavy noises. Wang et al. [72] proposed a Log-Gabor filter based fingerprint enhancement method. Comparing with Gabor filters, Log-Gabor filters can be constructed with arbitrary bandwidth which can be optimized to have minimal

spatial extent. For fingerprint enhancement, this unique property contributes significantly to improve the image quality. But due to the singularity in the log function at the origin, one can not construct an analytic expression for the shape of the Log-Gabor function in the spatial domain. Therefore, the filters are constructed in the frequency domain. Apparently, the original fingerprint image should be accordingly transformed to frequency domain for the implementation of the filter. Jang et al. [73] proposed an enhancement method based upon Half Gabor Filter (HGF) to reduce the computational cost of Gabor based approach. The HGF is a modified filter that reduces the mask size of Gaussian filter while preserving the frequency property of the Gaussian filter. The method proposed by Jang et al. is faster and saves memory space in comparison to the conventional Gabor Filter.

Willis et al. [74] proposed an FFT based fingerprint enhancement method. In this method the enhancement is achieved by multiplying the Fourier transform of the block by its power spectrum raised to a power k. The proposed method is computationally more expensive as large amount of overlap between adjacent blocks is required to avoid discontinuity at the edge between the adjacent blocks. S Chikkerur et al. [75] proposed an image enhancement algorithm based on Short Time Fourier Transform (STFT) analysis and contextual/ non-stationary filtering in Fourier domain. In the proposed method ridge orientation, frequency, angular coherence and region mask are probalististiclly estimated simultaneously using STFT analysis. The algorithm while reducing the space requirements in comparison also uses the full contextual information i.e. ridge orientation, frequency and angular coherence for enhancement. Some wavelet based fingerprint image enhancement [76, 77] methods have also been proposed in literature.

2.3.2.1.2 Segmentation

Segmentation is the decomposition of an image into its components. A captured image consists of two components known as foreground and background. The foreground regions correspond to the clear fingerprint area containing the ridges and valleys, which is the area of interest. The background corresponds to the noisy area outside the border of the fingerprint area, which do not contain any valid fingerprint information. So the function of the fingerprint segmentation is to separate the foreground region and the background region and to eliminate the background region. Segmentation is very important for the reliable

extraction of minutiae because without segmentation most feature extraction algorithms extract a lot of false features when applied to the noisy background area.

In the literature several approaches for fingerprint image segmentation are discussed. Mehtre et al. [78] proposed a method in which fingerprint area is classified according to the local histogram of ridge orientations**.** A histogram is computed for each 16×16 block and ridge orientation is estimated at each pixel. The orientation pattern is donated by the histogram peak while flat histogram donates the isotropic signal. This method fails when the input image has uniform blocks because no local ridge orientation can be found in those regions. Chatterjee et al. [79] modified the above method by assigning those blocks as backgrounds which have the gray scale variance lower than a particular threshold value. The above two methods suffer from the limitation of moderate segmentation performance. Ratha et al. [80] proposed another method in which each 16×16 block is classified as foreground or background according to the variance of gray levels in the orthogonal direction to the ridge orientation. Maio and Maltoni [67], proposed to classify fingerprint images as foreground or background by using the average magnitude of gradient in each image block. The gradient response is high in the foreground area due to ridge valley alteration in the fingerprint area and low in the background region. Shen et al. [81], convolved eight Gabor filters with each image block and used variance of filter response for fingerprint segmentation. Bazen et al. [82] proposed a pixel wise segmentation technique proposed in which coherence, mean and variance three pixel features are computed for each pixel. Then an optimal linear classifier is trained for the classification per pixel and morphology is applied to reduce the classification errors. Disadvantage of this algorithm is low speed and moderate performance. Chen et al. [83] used clusters degree, mean and variance for segmentation by means of an optimized linear classifier. The error rate for misclassified blocks is 2.45%. Klein et al. [84] computed gray mean, variance, gradient consistency and Gabor response for segmentation by using Hidden Markov Model (HMM). The performance of the model highly depends upon the choice of pixel features.

2.3.2.1.3 Binarization

Binarization is the process to convert a gray scale fingerprint image into a binary (black and white image).The easiest approach uses a global threshold works by setting the

pixels whose gray-level is lower than threshold to 0 and the remaining pixels to l [85]. A global threshold cannot be used as the different portions of the image may have different contrast and intensity. Another technique based upon the local threshold changes locally by considering the average local intensity. But the local threshold technique cannot guarantee acceptable results for images of poor quality. Stock et al. [86] proposed a composite approach based on a local threshold and a "slit comparison" formula that compares pixel alignment along eight discrete directions. Moayer et al. [87] proposed a binarization technique based on an iterative application of a Laplacian operator and a pair of dynamic thresholds. In each iteration, the image is convolved through a Laplacian operator and the pixels whose intensity lies outside the range bounded by the two thresholds are set to 0 and 1, respectively. Xiao et al. [88] proposed a method similar to Moayer et al. [87] but after the convolution step a local threshold is used to deal with regions of different contrast. In both the above techniques, repeated convolution operations are required which is a time consuming process. A fuzzy approach is proposed by Verma et al. [89]. This approach uses an adaptive threshold to preserve the same number of 1 and 0 pixels for each neighborhood. Ratha et al. [90] explained another binarization approach based on peak detection in the gray-level profiles along sections orthogonal to the ridge orientation. A 16×16 oriented window is extracted around each pixel. The gray-level profile is obtained by projection of the pixel intensities onto the central section. The profile is smoothed through local averaging, the peaks and the two neighboring pixels on either side of each peak constitute the foreground of the resulting binary image. The algorithm proposed by Ratha et.al. [90] is fast, but most of the bifurcations and even some ridges are broken by the oriented line segments. If the ridges are very close in the image, the binarized ridges are merged together. Emiroglu et al. [91] discussed a regional average thresholding (RAT) algorithm, which uses a 8×8 window but threshold only the 8×4 portion and slide the window for the next 4 points. Implementation of the RAT algorithm increases the processing time in comparison with a single threshold level algorithm but gives better results. In [92], Abutaleb et al. used genetic algorithm to discriminate ridges and valleys along the gray-level profile of scanned lines. The proposed optimization criterion is aimed at increasing the correlation between adjacent gray-levels along fingerprint sections. An adaptive binarization method proposed by Dong et al. [93] used the inter ridge distance to calculate the size of the neighborhood for each pixel. The

method of Onnia et al. [94] considers binarization as an optimization problem, which finds the best threshold that minimizes a weighted sum of square error function. Kheiri et al. [95] proposed a binarization algorithm in which the block size is optimized by calculating the statistical variance, and mean value of the intensity of a pixel of the block is used as a threshold value for that block. Zhang et al. [96] proposed an algorithm in which fingerprint image is divided into regions, each containing ridges that have similar ridge gray scale value and in order to store these regions a data structure has also been proposed. The binarization is then obtained by local thresholding.

2.3.2.1.4 Thinning

Thinning is the process of eroding the ridges of the fingerprint until they are one pixel wide. Thinning reduces the ridge pattern to a 1-pixel wide skeleton from which minutiae can easily be extracted [97, 98] as shown in Figure 2.3.

(a) (b)

Figure 2.3 Thinning (a) Original image (b) Thinned image

According to the elimination of pixels, the thinning algorithms are of two following types:

- Sequential
- Parallel

In sequential algorithms, the pixels are examined for deletion in a fixed sequence in any iteration. The deletion of a pixel in any iteration (say n^{th}) depends upon the results of $(n-1)^{th}$ iteration as well as on the pixels already processed in the n^{th} iteration. To prevent sequentially deletion of an entire branch in any iteration, a sequential algorithm marks all the

pixels to be deleted and all the pixels are removed at the end of the iteration. In parallel thinning algorithms a pixel satisfying a set of rules is immediately removed and deletion in n^{th} iteration depends only on the result that remains after $(n-1)^{th}$ iteration.

A good thinned image should have the following properties [99]

- Unit width – which means that obtained thinned image must be of single width.
- Connectivity- means that there should not be any discontinuity in the resulting image.
- Central axis- means that the resulting thinned ridges must be approximated to the medial axis.
- Noise elimination- means that any unwanted pixel including singular pixel (as they are not required by feature extraction stage in fingerprints) must be eliminated.

A fully parallel thinning algorithm that requires only a single pass per iteration has been proposed by Jang et al. [99]. The proposed algorithm requires a set of 20 elimination templates out of which 12 are 3 × 3, four are 4 × 4 and four 5 × 5. In addition to that the algorithm also requires 10 restoring templates of different sizes (three 3 × 3, three 4 × 3 and four 4 × 4). Since this algorithm requires with large neighbourhood information to ensure connectivity and performance with corners it consumes more time. Datta et al. [100] proposed a thinning algorithm which ensures some basic properties of thinning but the proposed algorithm uses multipass iterations and the algorithm is also not fully parallel and creates many spurious branches. A 2-sub iteration thinning algorithm with template matching is proposed by Zhang et al. [101]. The algorithm preserved the connectivity of the patterns and produces one pixel wide skeletons. The algorithm discussed above requires two sub iterations for thinning and is not fully parallel. Ahmed et al. [102] proposed a rule based rotation invariant thinning algorithm in which shape of the image is preserved because it thins the symbol to their central lines. The system has 20 rules which are applied simultaneously to each pixel. The algorithm is rotation invariant but it cannot remove the isolated points and the proposed algorithm is iterative in nature. Huang et al. [103] also proposed a rule base thinning algorithm, in which contour information is also added to overcome the problem of dis-connectivity and possible loss of information. The produced skeleton is close to the medial axis thus preserving the topology of the image. The proposed algorithm does not give one width skeletons, cannot remove isolated points and is not

rotation independent. A pixel array circuit for thinning has been proposed by Wang et al. [97]. The proposed thinning algorithm is based upon the Exclusive-OR, AND and OR logical operations between the pixels of a 3 × 3 window as shown in Figure 2.4.

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Figure 2.4 3×3 window

The algorithm uses two sub iterations and following conditions are examined:

a. $(X_1 \& X_2)+(X_2 \& X_3)+\ldots+(X_7 \& X_8)+(X_8 \& X_1)=0$

b. $(X_9 \oplus X_{11}) + (X_{10} \oplus X_{12}) \neq 0$

c. $X_{10}+X_{11}+ (X_9 \& X_{12}) = 0$

d. $X_9+X_{12}+(X_{10} \& X_{11}) = 0$

Where:

$X_i = (P_i \oplus P_{i+1}) ,\ldots\ldots..$ $i = 1,2,\ldots.8$ and $P_9 = P_1$;

$X_m = (P \oplus P_{(2n-1)}) ,\ldots\ldots$ $m = n+8$ and $n = 1,2\ldots..4$;

+ stands for Logical OR

& stands for Logical AND

$\oplus$ stands for Exclusive OR

In the first sub iteration conditions a, b and c are examined. If all of them are satisfied, the center pixel P as shown in Figure 2.4, will be reset to 0. In the second sub iteration, conditions a, b and d are checked. The signal of the center pixel P will remain as it is if any of the conditions is not satisfied. The proposed algorithm each pixel in the array needs only four connections with its neighbors and uses simple logic operations, so, it is easy to implement but the algorithm requires many iterations for the thinning process and does not generate images of unit width.

Luping et al. [104] proposed a parallel template based pulse coupled neural network based thinning algorithm. Under the control of pulse-coupled templates, this algorithm iteratively skeletonizes images using neuron pulses. It can preserve the basic image shape

and original connectivity without new breaks. A special direction-constraining scheme is applied to fingerprint image thinning via the orientation field, but the proposed algorithm is iterative in nature and requires much iteration for thinning.

2.3.2.2 Minutiae Extraction

The accuracy of the authentication system depends heavily on the capability of the feature extraction algorithm to extract the stable and accurate features. Reliable minutiae extraction is the key for the success of the minutiae based authentication system. Minutiae extraction methods can be divided into following two types:

- Direct gray-scale extraction methods
- Binarization based extraction methods

Direct gray-scale extraction methods do not require binarization and thinning. Many Direct gray-scale extraction methods are proposed in the literature. Leung et al. [105], introduced a neural network-based approach in which the image is first transformed into frequency domain where the filtering takes place and the resulting magnitude and phase signals constitute the input to the neural network composed of six sub-networks, each of which is responsible for detecting minutiae at a specific orientation. Finally a classifier is employed to combine the intermediate responses. Maio et al. [67] proposed a direct gray-scale minutia extraction technique based on the ridge line following algorithm. The ridge line following algorithm extract a ridge line, given a starting point and direction. The algorithm runs until ridge ending or bifurcation occurs or any one of other three stopping criteria becomes true. The system returns the type, coordinates and direction of the detected minutiae points. In the proposed algorithm the value of the ridge following step has been determined according to the average thickness of the ridge lines. Jiang et al. [106] proposed a modification to the method of Miao et al.. The proposed method uses the ridge information (ridge intensity variation and bending level) to find the ridge following step automatically. The low value of ridge intensity variation and bending level will result in larger ridge following step while a high value of these parameters will result in a small ridge following step. The proposed step will increase the speed of the system while the accuracy of the system will be less in comparison. Liu et al. [107] proposed another minutiae extraction algorithm which tracks a central ridge and two surrounding valleys simultaneously. During

the minutiae extraction process, the relationship between central maximum of the ridge and two minima of the corresponding valleys are monitored. Any change in the relationship indicates the presence of a minutia. In this method the ridge following step is calculated and adjusted automatically according to the distances between lateral minima from the central maximum. In [108], a method using Linear Symmetry (LS) properties computed by spatial filtering via separable Gaussian filters and Gaussian derivative filters is proposed by Nilsson and Bigun. Minutiae are identified in the gray-scale image as points characterized by the lack of symmetry i.e. minutiae are local discontinuities of the LS vector field.

In Binarization based methods the most commonly employed method of minutiae extraction is the crossing number (CN) concept. This method involves the use of the skeleton image where the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3×3 window of Figure 2.4. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood[109-112]. The CN for a ridge pixel *P* is given by

$$CN = 0.5\sum_{i=1}^{8}\left|P_i - P_{i+1}\right| , \qquad P_9 = P_1 \tag{2.4}$$

If CN = 1 then ridge pixel is a ridge ending, while if CN = 3 the ridge pixel is a ridge bifurcation otherwise it is a non-minutiae point. Crossing Number method registers minutiae to many such pixels which are not minutiae in actual and are required to be eliminated. Moreover, this method also considers minutiae to the boundary pixels.

2.3.2.3 Fingerprint Matching

Ideally, the minutiae extracted from the different impressions of the same fingerprint must match with each other but practically, due to displacement, rotation and other linear/ nonlinear distortions minutiae extracted from different impressions of the same fingerprint do not match with each other. In order to maximize the number of matching minutiae the alignment of the two fingerprints is required. After the pre-alignment process the matching process is simply a pairing process. Correctly aligning the fingerprints requires the translation and rotation between the two images, to be recovered exactly. Different approaches of fingerprint alignment proposed in the literature by the different authors have

been divided into absolute and relative pre-alignment. In absolute pre-alignment every fingerprint image is aligned, independently of the others, with respect to some reference point (core point, delta point etc.) or pattern before storing in the database. Wegstein [113] proposed a method which pre-aligns fingerprints with respect to core positions and average orientation of regions around the core point. Bazen et al. [114] described an absolute pre-alignment method based on the orientation of singularities. However, accurate and reliable detection of reference points is a difficult task especially in poor quality images. So, the pre-alignment errors due to inaccuracies involved in determining the reference point will cause the matching errors.

Jain et al. [115] proposed a relative pre-alignment approach in which ridges associated with minutiae are used to estimate the alignment. Each minutiae in a fingerprint is associated with a ridge, during the feature extraction stage when a minutia is recorded, the ridge corresponding to that minutia is also recorded. By matching these ridges in the reference and query image, the translation (Δx and Δy) and rotation ($\Delta\theta$) between the two images is estimated. The ridge matching task proceeds by iteratively matching pairs of ridges until a pair is found whose matching degree exceeds a certain threshold. The minutiae associated with the two matched curves are used as a reference points and the remaining minutiae are converted to polar coordinates. The converted minutiae are translated into symbolic strings and the correspondence between the minutiae is then obtained by dynamic programming algorithm that finds the minimum edit distance between the strings. This approach is capable of compensating for the alignment to some extent. However, the size of the template has to be large which require more memory and is more computationally expensive. Luo et al. [116] proposed a slightly different method in which instead of correlating the y coordinates of the sampled points along the two ridges, the distances and relative angles of the sampled points are matched. Zhang et al. [117] explored the possibility of using core points for relative alignment. In the proposed algorithm the core points from the two fingerprints are detected using multi resolution algorithm and are used to calculate the translation parameter. Structural features of minutiae close to the core point are computed and are used to determine the rotation parameter. This is a fast approach of fingerprint alignment but the system fails in case of plain arches or images that do not have core points. Moreover, the performance of the system degrades for low quality fingerprints. Feng et al.

[118] proposed another approach which uses one minutia and several associated ridges to align two fingerprints. This is accomplished by firstly defining a substructure that contains as much local information (one minutia and several ridges) as possible, and secondly by finding the substructure pair which have the most consistent substructure pairs around. The proposed algorithm uses the information in the local area and estimate deformation more accurately but the proposed alignment algorithm is required to be improved for fingerprints with fewer minutiae and is computationally expensive. In the method proposed by Hu et al. [119], eight types of special ridges have been introduced to align two fingerprints. The ridge with maximum of sampled curvature has been used as reference ridges for initial alignment and other corresponding ridges have been aligned using different features. The alignment parameters of translation and rotation finally come from all aligned special ridge pairs. The proposed method shows some improvement over minutiae based method but is dependent upon the preprocessing steps such as thinning, enhancement etc.. Zhao et al. [120] proposed another technique for alignment of partial high resolution fingerprints using pores. In the proposed method after pore detection, a pore-valley descriptor (PVD) has been defined to describe pores based on their local characteristics. Then a coarse-to-fine pore matching method has been used to find the pore correspondences based on PVD. With the detected corresponding pores, the alignment transformation between the fingerprint fragments has been estimated. The PVD-based method can accurately detect the corresponding feature points and hence estimate better alignment transformation, but, this method from the problem that all pores will not appear in the fingerprint images of the same person which are captured at different times. Other problem of this method is the expensive computational cost caused by the large amount of pore features.

A wide variety of fingerprint matching techniques have also been proposed in the literature. Chen et al. [121] proposed a topology based matching algorithm for fingerprint authentication in which the structure of the fingerprint is represented by a geometrical configuration of its minutiae, thus reflecting the general spatial structure in the neighborhood of each minutiae. After the minutiae have been extracted, a specific neighborhood, called the minutiae window is determined for each of them. This information is used to find candidate minutiae from each set that are potential matches. Starting from a minutia in one set, a tree is grown with minutiae as the tree nodes. After an edge is added the other minutiae set is

examined to see if a similar edge can be added. This process continues until the tree is sufficiently large or no more edge can be added to both sets. The scheme is based upon the assumption that the surrounding features of closed neighborhood are supposedly invariant to rotation and translation. Moreover minutiae associated with whorls, noisy region creates troublesome. Spurious and missing minutiae further degrade the system.

Hybrid matching algorithms using both local and global features are proposed in [122-124]. Jain et al. [122] proposes a method capturing both the local and global features into a so-called FingerCode, using a bank of Gabor filters. The matching is then reduced to finding the Euclidean distance between these FingerCodes and hence it shall be very fast and the rotation invariance can be easily achieved. But, this representation and matching scheme assume that the reference point can be determined with a reasonable accuracy, which is not a trivial task. This scheme also does not take into account a significant nonlinear elastic distortion in the fingerprint. Jain et al. [123] proposes another hybrid matching algorithm that uses both minutiae (point) information and Texture (regional) information for matching the fingerprints. The hybrid method leads to a substantial improvement in the over all matching performance but non linear deformation present in the fingerprint images have not been accounted for in this method. Huvanandana et al. [124] proposed another hybrid system for automatic finger identification with a fast filters based searching and a minutiae matching. This method needs fewer steps to identify individuality than tradition methods but the accuracy of fingerprint classification is less in this method. Jia et al. [125] proposed a minutia method based on the vector triangle. This method incorporates the information of ridge lines into the process of determining the reference points in two fingerprint images and realizes the fingerprint matching in the polar coordinate system. This method does not rely on the core points and is invariant to rotation and small amount of scale changes but this system gives errors for images of poor quality. Ceguerra et al. [126] proposed a new approach for combining the local and global recognition schemes for automatic fingerprint verification by using matched local features as the reference axis for generating global features. They combined the minutia based and shape based techniques. The integrated scheme gives the average performance. However by combining the better local and global recognition schemes this performance can be improved. P Bhowmick et al. [127] proposed a new technique of fingerprint matching using an efficient data structure, combining the minutiae representation

with the individual usefulness of each minutia to make the matching more powerful. This method uses the local topological structure of a valid minutiae and the global structure of the minutiae as a whole. The improvements in execution time and FAR are still possible.

2.4 Multibiometric

The dictionary meaning of multi is more than one or many. In multi biometric system more than one source of information are combined together to form a combined system in order to overcome the limitation of single biometric system. The source of information in multi biometric system, when multiple source of information is derived from the same biometric trait, may include:

(i) Multiple sensors to capture the same biometric trait (e.g. capturing fingerprint image using optical and solid sensors)

(ii) Multiple algorithm for the same biometric trait (e.g. texture and minutiae based algorithm for fingerprints)

(iii) Multiple samples of same biometric trait (e.g. more than one impression of the same finger of the person)

(iv) Multiple instances of same biometric trait (e.g. fingerprint image of the two different fingers of the same person)

When the information is derived from the different biometric traits the same is known as multimodal biometric system. Fingerprints are often combined with other biometric traits to form a multimodal system. The combined system is likely to produce a system that is usable by a large population because a small fraction of the population that cannot use fingerprint biometric due to hand related disabilities or due to poor quality fingerprints, may be given the option to use the another biometric combined with the fingerprints. Moreover, the combined system will be more robust to impostor attacks and it will not be easy to circumvent the system because the chances of stealing all the biometric of a person at the same time are very less. In addition, a multimodal system can be used to know the presence of the authorized person by asking the user to present the different biometric trait in random order. A large number of studies have been performed combining the fingerprints with other biometric modalities as given in Table 2.1.

Table 2.1 Different biometric modalities combined with fingerprints

Sr. no.		Authors	Year	Reference no.	Biometric trait(s) fused with fingerprint
1.	a)	L. Hong and A. K. Jain	1997	[128]	Face
	b)	L. Hong and A. K. Jain	1998	[129]	
	c)	A. K. Jain, L. Hong and Y. Kulkarni	1998	[130]	
	d)	M. Indovina, U. Uludag, R. Snelick, A. Mink and A. K. Jain	2003	[131]	
	e)	R. Snelick, U. Uludag, A. Mink, M. Indovina and A. K. Jain	2005	[132]	
	f)	D. Bouchaffra and A. Amira	2008	[133]	
	g)	T. Sim, S. Zhang, R. Janakiraman and S. Kumar	2007	[134]	
	h)	A. Patra and S. Dass	2008	[135]	
2.		A. K. Jain, L. Hong and Y. Kulkarni	1999	[136]	Face and speech
3.	a)	A. Ross, A. K. Jain and J. Qian	2001	[137]	Face and hand geometry
	b)	A. Ross, A. K. Jain	2003	[138]	
4.		J. F. Angular, D. G. Romero, J. O. Garcia and J. Gonzalez	2005	[139]	Signature
5.		K. A. Toh, W. Xiong, W. Y. Yau and X. Jiang	2003	[140]	Hand geometry
6.	a)	Y. Wang, Y. Wang and T. Tan	2004	[141]	Voice
	b)	K. A. Toh and W. Y. Yau	2004	[142]	
	c)	K. A. Toh and W. Y. Yau	2005	[143]	
7.	a)	A. K. Jain, S. C. Dass and K. Nandkumar	2004	[144]	Soft biometrics
	b)	A. K. Jain, S. C. Dass and K. Nandkumar	2004	[145]	

7.	c)	H. Ailisto, E. Vildjiounaite, M. Lindholm, S. M. Makela and J. Peltola	2006	[146]	Soft biometrics
8.		A. K. Jain, K. Nanadakumar, X. Lu and U. Park	2004	[147]	Face and soft biometrics
9.		S. Ribaric and I. Fratric	2005	[148]	Palmprint
10.		A. Kumar and D. Zhang	2006	[149]	Palmprint and hand geometry

2.4.1 Level of Fusion

The process of combining the evidences provided by different biometric sources is known as biometric fusion. Depending upon the type of information that is required to be fused, the fusion scheme can be classified into following four categories:

(i) Sensor or signal level fusion

(ii) Feature level fusion

(iii) Score level fusion

(iv) Decision level fusion

In sensor the fusion the raw data from different sensors is combined together [150]. Maximum information content is available at this stage but the raw data from different information sources must be compatible and their interrelationship must be either known in advance or can be reliably estimated. So, the sensor level fusion can be performed in a system where the information sources use samples of the same biometric trait obtained from either multiple compatible sensors or multiple instances using a single sensor. For example, mosaicking of multiple fingerprint impressions to form a more compatible fingerprint image [151 -155].

In feature level fusion features extracted from different information sources are combined to form a joint feature vector. Like sensor level fusion, the feature level fusion is also used for combining multiple feature sets from the same finger. Feature sets form different biometric modalities may be concatenated to form a single feature set, provided the feature sets are compatible. Some examples of feature level fusion are explained in the

literature by the different authors [156-158]. Integration at feature level is difficult to achieve because the relationship between the feature spaces of different biometric sources may not be known and feature set may be incompatible. Moreover, concatenating two feature vectors will result in a feature vector with large dimensionality which may lead to the curse of dimensionality problem [159].

Score level fusion is commonly preferred method in multibiometric systems [160]. It is relatively easy to access and combine (than sensor and feature) the match scores generated by different biometric matching stages but the information content is less than sensor and feature level fusion. In fact, score level fusion is best tradeoff between effectiveness and ease of fusion. Moreover, this type of fusion can be implemented in all type of biometric fusion scenarios. Integration at score level requires some attention in the sense that the output of the individual matchers may be in the different range or may follow different probability distributions [160].

In decision level fusion the output of the individual biometric systems are combined to take the final decision. In a verification system each individual systems returns a match or no match (binary decision) so, the obvious decision level fusion methods are AND and OR rule [161], majority voting [162], weighted majority voting [163] based methods. One advantage of these methods is that they are easy to explain and implement. The AND and OR decision level fusions are duals of each other. AND results in lowering the False Match Rate (FMR) and increases the False Non Match Rate (FNMR) while OR results in lowering the FNMR and increases the FMR. Fusion at decision level is simple but the accuracy of the output depends on the accuracy of the individual components of the system working independently.

2.5 Summary

Although, lot of work has been done in the field of fingerprint authentication, still fingerprint authentication is not a fully solved problem. There are still many challenges in designing completely reliable and automatic fingerprint system. In the preprocessing stage of minutiae based system many thinning algorithms have been proposed but still there is a need to design a thinning algorithm that not only produce a thinned image of one pixel width but also preserves the connectivity of the image and consumes very less time. In the feature

extraction stage crossing number is the commonly used and widely accepted binarization algorithm of minutiae extraction but this method is not robust against spikes (false minutiae) and register many points as ridge ending or bifurcations points although in actual they are not minutiae points so there is a need to modify this algorithm in order to extract reliable features from the fingerprints. Moreover, during fingerprint matching more robust fingerprint alignment algorithms are required which may be developed using soft / evolutionary computational techniques that perform the required function accurately.

The single biometric alone sometimes cannot meet all the security requirements of the modern day transactions due to intra class variations, noise, non uniqueness etc. So, for high security requirements multibiometric or combined strategy of biometric and conventional methods is the need of the hour.

CHAPTER 3

Minutiae Based Fingerprint Authentication System

Minutiae based fingerprint authentication systems rely on local discontinuities in the ridge flow pattern i.e. ridge endings and ridge bifurcations. The locations and angular orientation of the ridge endings and ridge bifurcations within the fingerprint uniquely characterize the fingerprint. The present chapter includes improved methods for preprocessing of fingerprint image, minutiae extraction and genetic algorithm (GA) based relative alignment. A comprehensive comparison of the results of improved methods with the existing methodologies has also been presented in this chapter.

In minutiae based authentication system the various steps required to find the out the authenticity of the person are:

i) Preprocessing
ii) Feature Extraction (Minutiae Extraction)
iii) Post processing
iv) Alignment and validation

3.1 Preprocessing

Preprocessing of the fingerprint image is a critical step in an automatic fingerprint authentication system in order to reliably extract minutiae from the input fingerprint image. In order to eliminate unwanted information and to prepare the image for feature extraction, preprocessing of the signal is required. Various steps for preprocessing used in this work are:

- Segmentation
- Binarization
- Thinning

Segmentation is the decomposition of an image into foreground (area of interest) and background. Various segmentation algorithms present in the literature [78-84] have been discussed in the previous chapter.

In the present work, segmentation is performed by calculating the variance and mean. A foreground region has a high variance value while a background region has low variance value. The image is divided into a W×W window size and variance of each window is calculated. If the variance is below a particular value (threshold) `then it is a background. If it is above a particular value then it contains information. The variance window k of size W × W is given by

$$\sigma^2(\mathrm{k}) = \frac{1}{W^2}\sum_{i=0}^{W-1}\sum_{j=0}^{W-1}\left(I(i,j) - M(k)\right)^2 \qquad (3.1)$$

Where M(k) = Mean of block k

I(i, j) = Value at pixel (i, j)

The choice of threshold value of variance and the window size W × W is very critical. Experiments have been conducted on a number of images of FVC2002/Db1_a database using the different threshold values and different window sizes. It has been observed that too low value of variance (threshold) leaves the background pixels while too high value of threshold distorts the image. It has also been observed that with too low and too high size of the window the image gets distorted. A threshold value of variance 75 and window size 16 × 16 gives good results. So, these two values have been used in the present work.

For the purpose of binarization Regional Average Thresholding (RAT) algorithm proposed in [91] has been used. The algorithm of RAT operates in the following stages:

i) Divide the image into windows of 8×8 pixels

ii) Calculate the average of the gray level in the first window

iii) Threshold the leftmost region (8×4) by using the average gray level calculated in stage 2

iv) Move the 8×8 window by 4 pixels to the right.

Repeat stage ii) to iv) until whole image is processed.

The comparison of Global thresholding and Regional Average Thresholding (RAT) has been shown in Figure 3.10.

Thinning is one of the most important components of fingerprint identification/verification system. A good thinned image can facilitate the reliable feature extraction and hence the authentication of a person. An improved and efficient thinning algorithm has been proposed with modifications in the algorithm suggested by Huang et al.

[103]. In the proposed algorithm the 8 neighbors of a pixel in a 3×3 window are arranged as 8 bits of a byte and corresponding Hexadecimal (Hex) value is calculated. These Hex values are used to obtain a minimized Boolean expression, using standard Karnaugh Map (K map) technique. The proposed algorithm results in better thinned images. Three implementation steps have also been proposed to speed up the thinning process.

3.1.1 Proposed Thinning Algorithm

The process of thinning begins with eliminating the pixels that lie on the outer boundary of the ridge until the ridge is one pixel wide. In a thinning algorithm two types of rules are required-

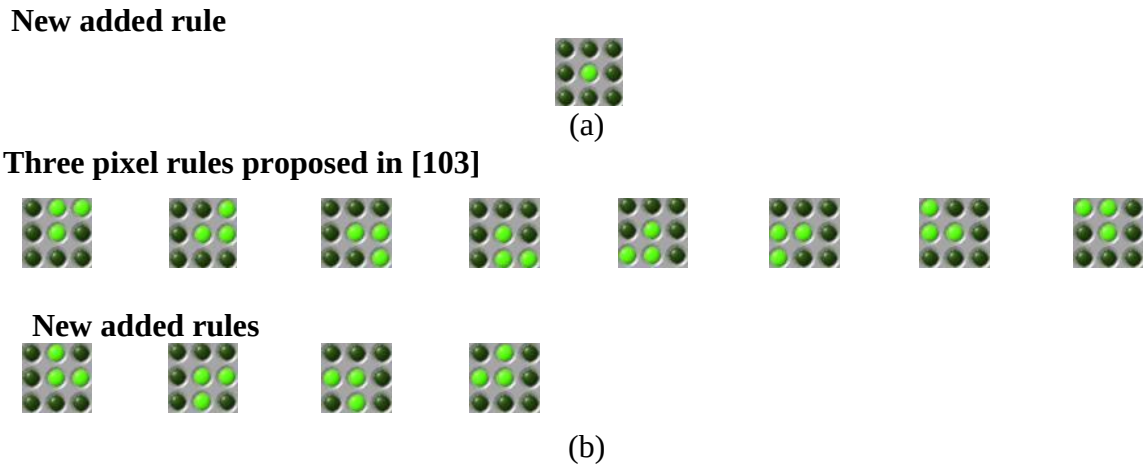
- Rules for elimination of a pixel
- Rules for preservation of a pixel (to ensure connectivity)

For the elimination process, a 3×3 window has been considered as shown in Figure 3.1.

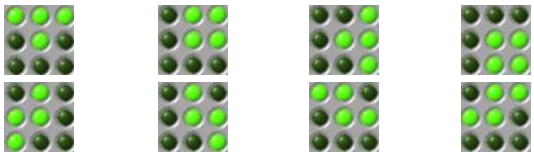
P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Figure 3.1 3×3 Operation window

All 256 combinations of neighboring 8 pixels of the central pixel are examined. A set of combinations is then selected for elimination and these combinations are given in the Figure 3.2.



Four pixel rules proposed in [103]



New added rules

(c)

Five pixel rules proposed in [103]

New added rules

(d)

Six pixel rules proposed in [103]

(e)

Seven pixel rules proposed in [103]

(f)

Eight pixel rules proposed in [103]

(g)

Figure 3.2 Conditions for elimination of a pixel

Figure 3.2 (a) to 3.2 (g) represents the different conditions under which the pixel is to be eliminated. These figures are differentiated according to the number of 1s (green pixels) around the central pixel in a 3×3 window.

New rules have been added to the rules proposed in [103] as shown in Figure 3.2. The singular points are removed, as they are not required in the minutiae extraction stage of

fingerprints. The rules have been added to make the elimination symmetric and rotation independent. This step has improved the resulting thinned image because main problem in finger print authentication is that of translation and rotation of the fingerprint image.

The templates for preservation of pixel are used to avoid any loss of connectivity of the thinned image. The preservation rules are used as proposed in [103] and is given in Figure 3.3.

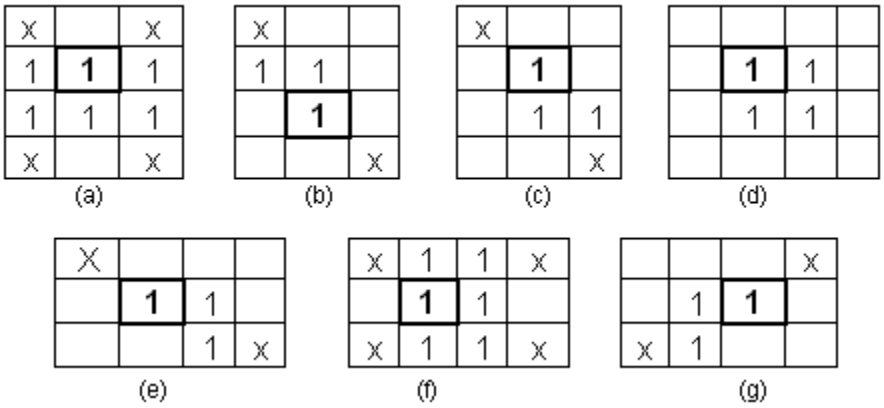


Figure 3.3 Templates for preservation of pixel as proposed by Huang et al. [103]

In order to speed up the process three implementation steps have been used. These are-

- Extraction of a single 5×5 window instead of extracting 3×3, 4×3 and 4×4 templates separately as proposed in [103] to check the preservation of the pixel. Extracted window as shown in Figure 3.4 is used to check simultaneously all the condition given in Figure 3.

s	t	u	v	w
r	f	g	h	x
q	e	P	a	i
z	d	c	b	j
o	n	m	L	k

Figure 3.4 5×5 window around the pixel P in question

The Logical expression for the preservation of a pixel is given by the following expression Y=(a&b&c&d&e&~g&~m)+(g&f&~a&~c&~d&~e&~u&~v)+(b&c&~d&~e&~g&~h&~a&~m&~n)+(a&b&c&~d&~e&~f&~g&~h&~i&~j&~k&~l&~m&~n&~y)+(a&b&~c&~d&~e&~g&~h&~i&~y)+(a&g&h&b&c&~i&~e)+(~a&~b&~c&d&e&~f&~g&~q&~r);

Where: &, + and ~ represents Logical AND, Logical OR and Logical NOT operations respectively.

If Y =

This process improves the time required for window extraction.

- Arranging the 8 neighbour of a pixel as 8 bits of a byte to calculate the Hex value as shown in the Figure 3.5 (instead of calculating the weight values of the eight neighbouring pixels and using the look up table to decide the elimination of a pixel as given in [103]).

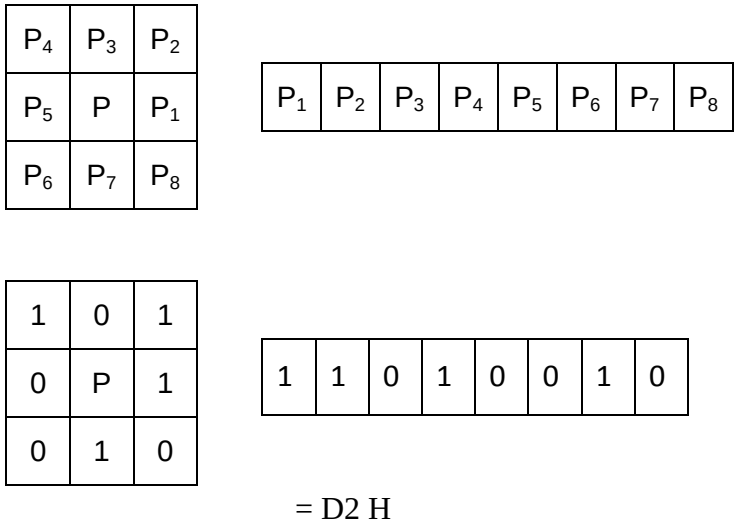


Figure 3.5 Calculation of Hexadecimal value

Table 3.1 shows the truth table of all the conditions required for the elimination of a pixel for thinning.

Table 3.1 Truth table of elimination rules for thinning

P_1	**P_2**	**P_3**	**P_4**	**P_5**	**P_6**	**P_7**	**P_8**	**Hex. Value**
0	0	0	0	0	0	0	0	00
0	1	1	0	0	0	0	0	60
1	1	0	0	0	0	0	0	C0
1	0	0	0	0	0	0	1	81
0	0	0	0	0	0	1	1	03
0	0	0	0	0	1	1	0	06
0	0	0	0	1	1	0	0	0C

0	0	0	1	1	0	0	0	18
0	0	1	1	0	0	0	0	30
1	0	1	0	0	0	0	0	A0
1	0	0	0	0	0	1	0	82
0	0	0	0	1	0	1	0	0A
0	0	1	0	1	0	0	0	28
0	1	1	1	0	0	0	0	70
1	1	1	0	0	0	0	0	60
1	1	0	0	0	0	0	1	C1
1	0	0	0	0	0	1	1	83
0	0	0	0	0	1	1	1	07
0	0	0	0	1	1	1	0	0E
0	0	0	1	1	1	0	0	1C
0	0	1	1	1	0	0	0	38
0	0	1	0	1	1	0	0	2C
0	1	0	0	0	0	1	1	43
1	0	1	1	0	0	0	0	B0
0	1	1	0	1	0	0	0	68
1	0	0	0	0	1	1	0	86
0	0	0	1	1	0	1	0	1A
1	1	0	0	0	0	1	0	C2
0	0	0	0	1	0	1	1	0B
1	1	1	1	0	0	0	0	F0
1	1	1	0	0	0	0	1	E1
1	1	0	0	0	0	1	1	C3
1	0	0	0	0	1	1	1	87
0	0	0	0	1	1	1	1	0F
0	0	0	1	1	1	1	0	1E
0	0	1	1	1	1	0	0	3C
0	1	1	1	1	0	0	0	78
1	0	1	1	0	0	0	1	B1
0	1	1	0	1	1	0	0	6C
1	1	0	0	0	1	1	0	C6
0	0	0	1	1	0	1	1	1B
1	1	1	1	0	0	0	1	F1
1	1	1	0	0	0	1	1	E3
1	1	0	0	0	1	1	1	C7
1	0	0	0	1	1	1	1	8F
0	0	0	1	1	1	1	1	1F
0	0	1	1	1	1	1	0	3E
0	1	1	1	1	1	0	0	7C
1	1	1	1	1	0	0	0	F8
1	1	1	1	0	0	1	1	F3
1	1	1	0	0	1	1	1	E7
1	1	0	0	1	1	1	1	CF

1	0	0	1	1	1	1	1	9F
0	0	1	1	1	1	1	1	3F
0	1	1	1	1	1	1	0	7E
1	1	1	1	1	1	0	0	FC
1	1	1	1	1	0	0	1	F9
1	1	1	1	1	1	0	1	FD
1	1	1	1	0	1	1	1	F7
1	1	0	1	1	1	1	1	DF
0	1	1	1	1	1	1	1	7F

All the Hex values are combined to obtain a simplified Boolean expression using standard Karnaugh Map (K-Map) technique. The K-Map thus obtained for all the conditions of eliminating the pixel is shown in the Figure 3.6.

	0000	0001	0011	0010	0110	0111	0101	0100	1100	1101	1111	1110	1010	1011	1001	1000
0000	1	0	1	0	1	1	0	0	1	0	1	1	1	1	0	0
0001	0	0	0	0	0	0	0	0	1	0	1	1	1	1	0	1
0011	1	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1
0010	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1
0110	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1
0111	1	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1
0101	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1100	1	1	1	1	1	1	0	0	0	0	1	0	0	0	0	0
1101	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
1111	1	1	1	0	0	1	0	0	1	1	0	0	0	0	1	1
1110	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0
1010	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1011	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1001	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
1000	0	1	1	1	1	1	0	0	0	0	1	0	0	0	0	0

Figure 3.6 Karnaugh map for the elimination rules for thinning

- Applying the short circuit AND (&&) and OR (||) operators available in the MATLAB instead of using simple AND (&) and OR (|) logical operators. Short circuit operators evaluate the second operand only when the result is not fully determined by the first operand and thus speed up the whole operation.

Figure 3.7 shows the flow chart of proposed thinning algorithm.

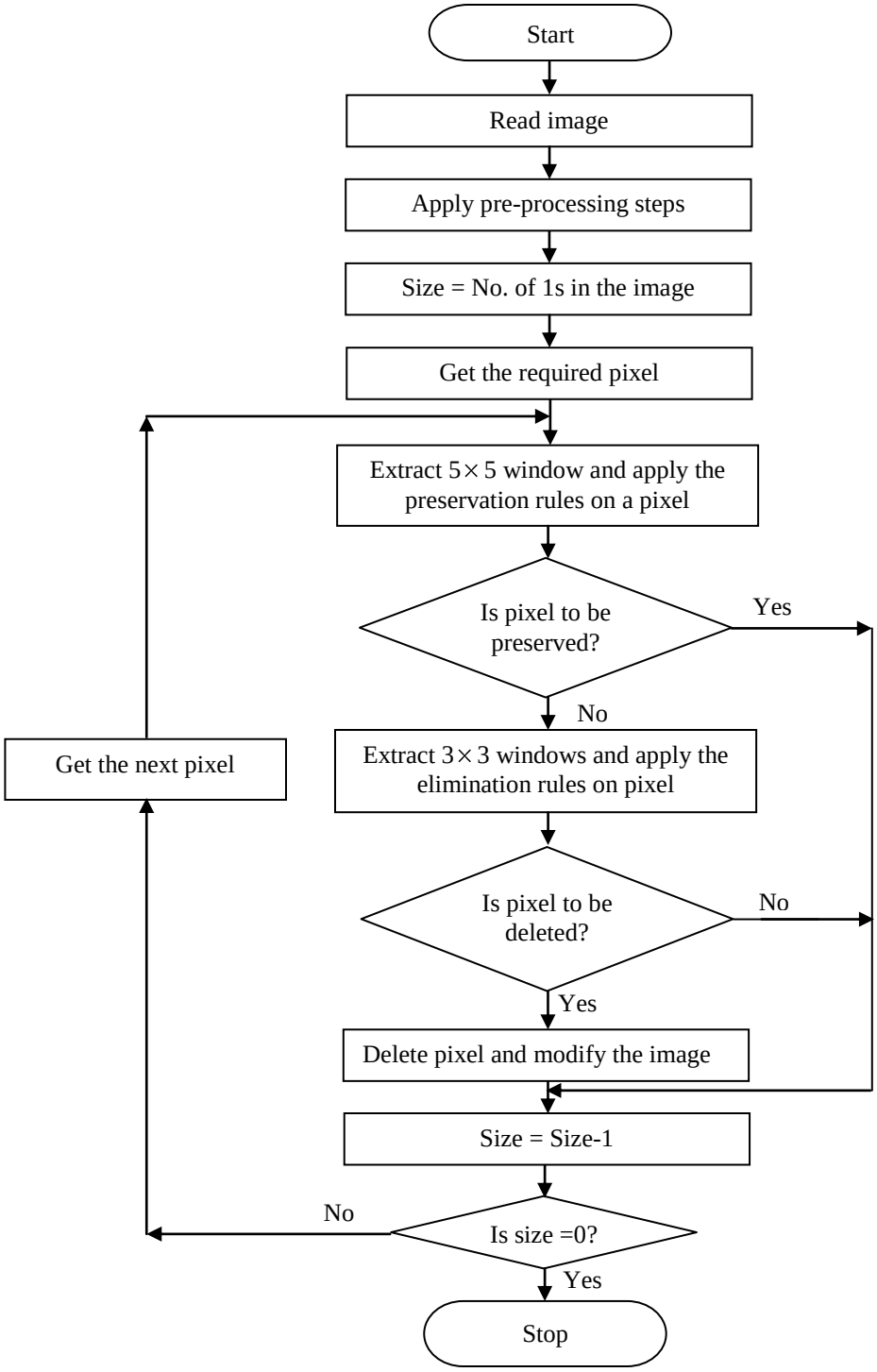


Figure 3.7 Flow chart of the proposed thinning algorithm

3. 1.1.1 Results and Comparisons of Thinning Algorithms

The above thinning algorithms have been developed in MATLAB version 7.0 on Pentium D CPU 2.80 GHz, 1GB of RAM. On comparing the proposed algorithm with the algorithm proposed in [103] it has been observed that the proposed algorithm is superior to the later. As shown in Figure 3.9 the proposed algorithm results in entire one pixel width thinned image in comparison to the two pixel width image resulted from the Huang et al. algorithm. The Figure 3.8 represents the original image on which thinning algorithms has been applied.

Figure 3.8 Original image for thinning

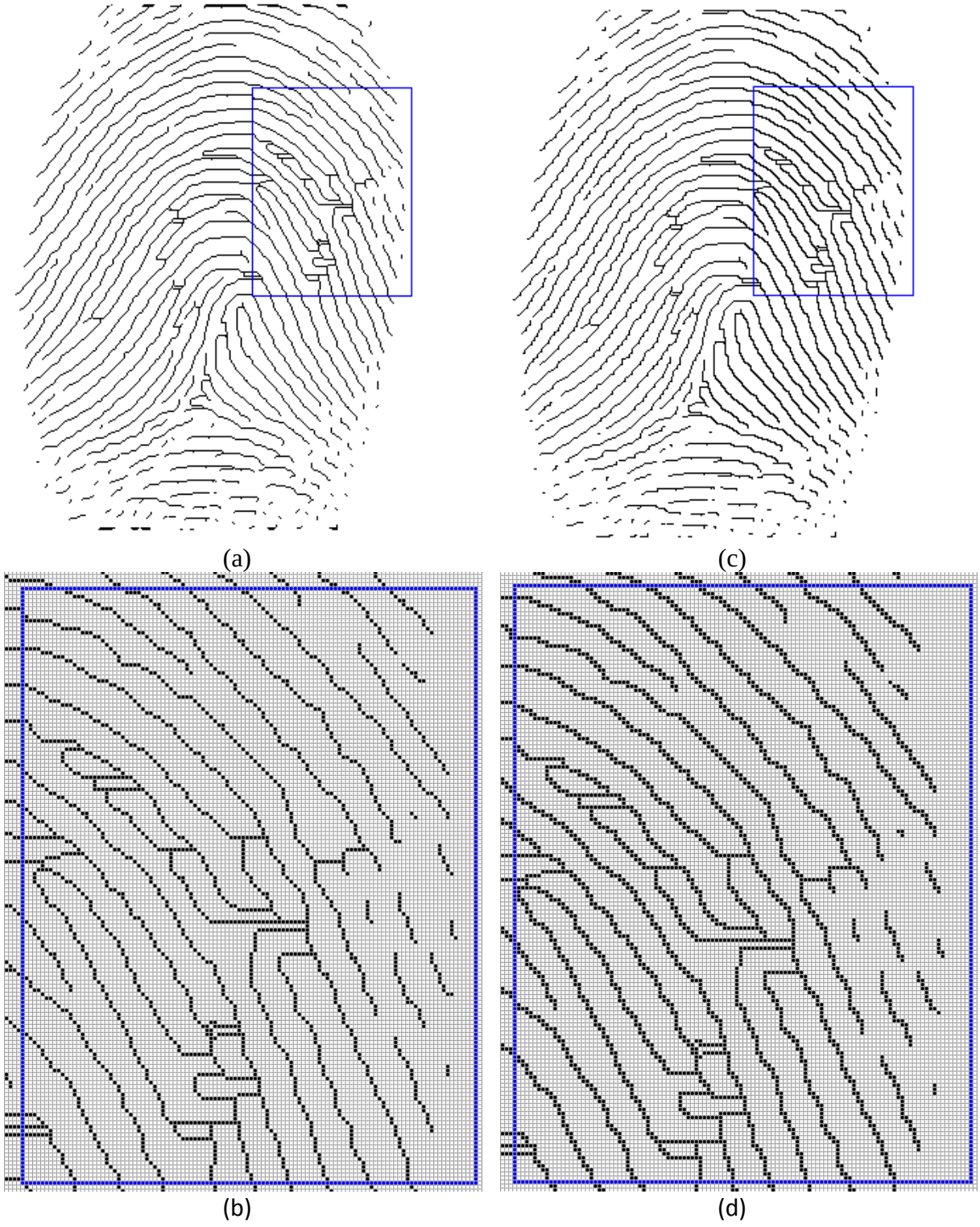


Figure 3.9 (a), (b) Thinned image & expanded portion of thinned image of proposed method with global thresholding (c), (d) Thinned image & expanded portion of thinned image Huang et al. method with global thresholding

Figure 3.10 represents the effect of global and regional average thresholding algorithms on the thinned images.

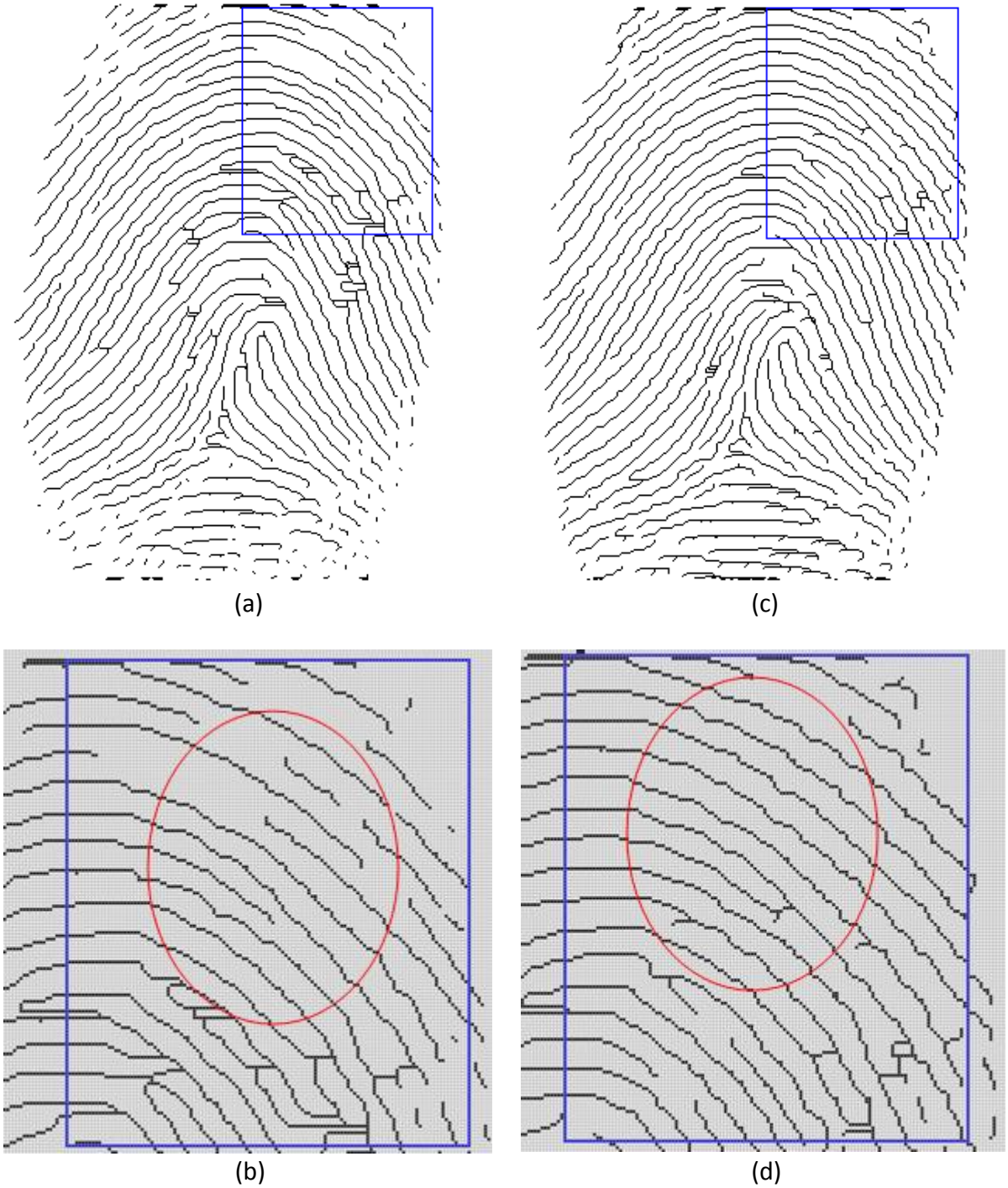


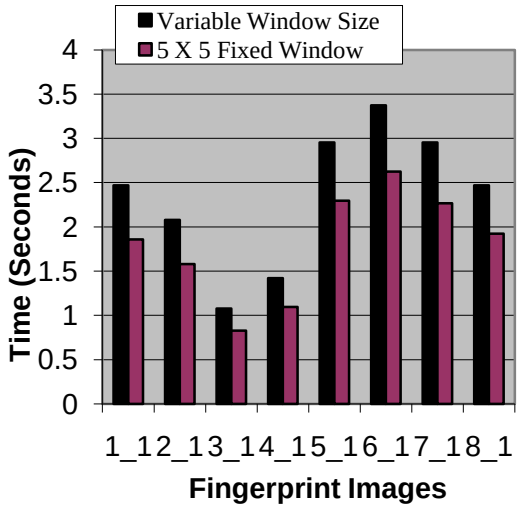
Figure 3.10 (a), (b) Thinned image & expanded portion of thinned image of proposed method with global thresholding (c),(d) Thinned image & expanded portion of thinned image of proposed method with regional average thresholding

The results of the three proposed implementation steps are given in Table 3.2, 3.3 and 3.4. All the tables show the actual implementation (CPU) time of the algorithms in seconds. As observed from the Table 3.2 the extraction of 5×5 window result in reduction of time by 22% in comparison to the time taken by extracting variable i.e. 3×3, 4×3 and 4×4 size window.

Table 3.2 Comparison of CPU time (seconds) for variable size window and 5×5 window

Figure No.	CPU Time (Seconds)		% Reduction in time
	Variable Window Size	Window 5×5	
1_1	2.469	1.859	**24.71**
2_1	2.078	1.578	**24.06**
3_1	1.078	0.828	**23.19**
4_1	1.422	1.094	**23.07**
5_1	2.953	2.297	**22.21**
6_1	3.375	2.625	**22.22**
7_1	2.953	2.266	**23.26**
8_1	2.469	1.922	**22.15**

(a)

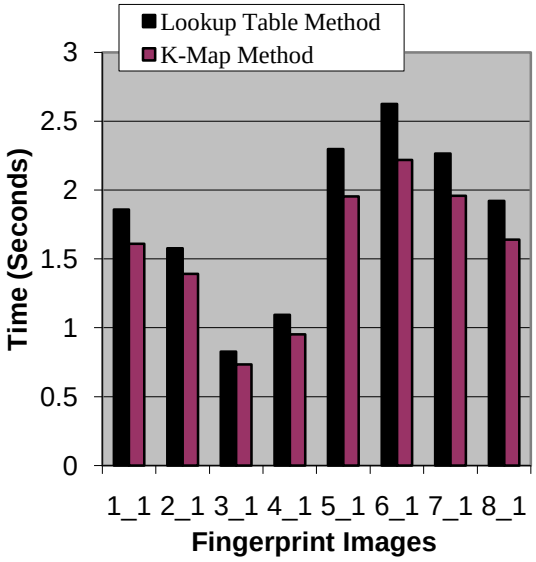


(b)

Table 3.3 Comparison of CPU time (seconds) for Lookup table method and K-map method

Figure No.	CPU Time (Seconds)		% Reduction in time
	Lookup Table method	K-Map method	
1_1	1.859	1.609	**13.45**
2_1	1.578	1.391	**11.85**
3_1	0.828	0.734	**11.35**
4_1	1.094	0.953	**12.89**
5_1	2.297	1.953	**14.98**
6_1	2.625	2.219	**15.47**
7_1	2.266	1.958	**13.59**
8_1	1.922	1.641	**14.62**

(a)



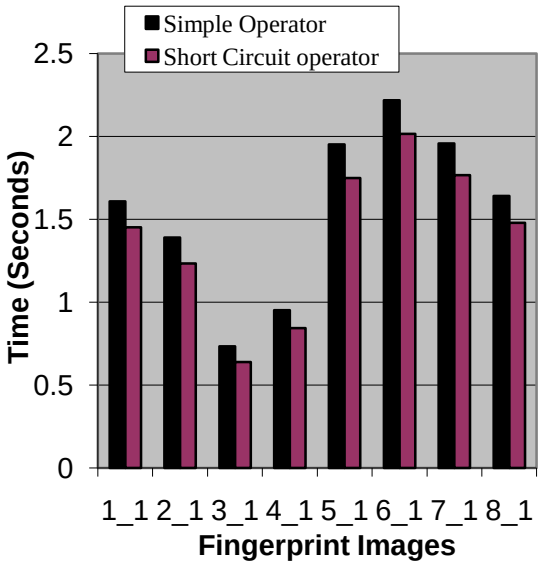
(b)

Table 3.3 shows the superiority of the K-Map technique over the lookup table method. A reduction of more than 10% in time has been achieved by implementing the simplified Boolean expression using K-Map having 5×5 window. The time further reduced by using the short circuit logical operators available in MATLAB instead of simple logical operators as shown in the Table 3.4.

Table 3.4 Comparison of CPU time (seconds) for simple and short circuit logical operators

Figure No.	CPU Time (Seconds) Logical Operators		% reduction in time
	Simple	Short circuit	
1_1	1.609	1.453	**9.70**
2_1	1.391	1.235	**11.21**
3_1	0.734	0.640	**12.81**
4_1	0.953	0.844	**11.44**
5_1	1.953	1.750	**10.39**
6_1	2.219	2.016	**9.15**
7_1	1.958	1.766	**9.81**
8_1	1.641	1.480	**9.81**

(a)

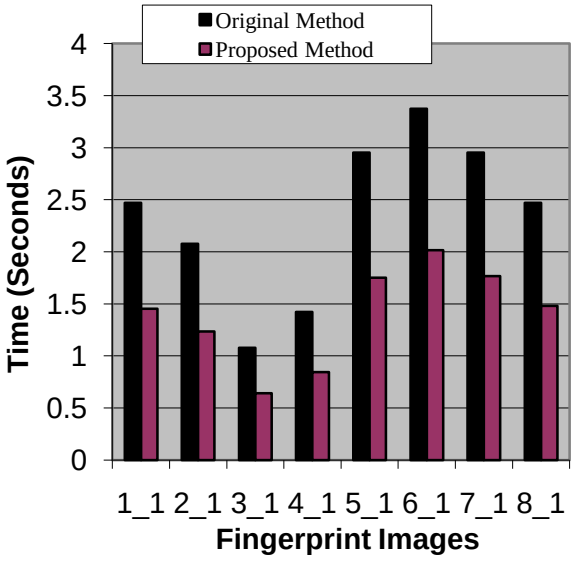


(b)

Table 3.5 Comparison of CPU time (seconds) for Huang et al. method [103] and proposed method

Figure No.	CPU Time (Seconds)		% Reduction in time
	Huang et al. method[24]	Proposed method	
1_1	2.469	1.453	**41.15**
2_1	2.078	1.235	**40.57**
3_1	1.078	0.640	**40.63**
4_1	1.422	0.844	**40.65**
5_1	2.953	1.750	**40.74**
6_1	3.375	2.016	**40.27**
7_1	2.953	1.766	**40.20**
8_1	2.469	1.480	**40.06**

(a)



(b)

As indicated in the Table 3.5 the overall enhancement in speed of about 40%, in the implementation of algorithm has been achieved.

3.2 Feature Extraction

Features (Minutiae) are extracted from the fingerprint in question and are compared with the features of the reference image already stored in the database for authentication. Crossing number (CN) is the most commonly used minutiae extraction method in fingerprints. The CN for a ridge pixel *P* is given by [109-112]

$$CN = 0.5\sum_{i=1}^{8} \left| P_i - P_{i+1} \right| , \qquad P_9 = P_1 \tag{3.3}$$

If CN = 1 then ridge pixel is a ridge ending, while if CN = 3 the ridge pixel is a ridge bifurcation otherwise it is a non-minutiae point. Crossing number method is not robust against the spikes (false minutiae) and tends to register spike as minutiae, which is required to be eliminated in post processing. In this work, a new method of minutiae extraction has been proposed which eliminates the spikes (false minutiae) as well as the boarder pixels.

3.2.1 Proposed Method of Minutiae Extraction

In the proposed method ridge ending and ridge bifurcation (minutiae) are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3×3 window of Figure 3.1. The 8 neighbors of a pixel in a 3×3 window are arranged as 8 bits of a byte and corresponding hexadecimal (Hex) value is calculated. These Hex values are simplified using standard Karnaugh Map (K map) technique to obtain the minimized logical expression.

3.2.1.1 Ridge Ending

All 2^8 = 256 cases 8 surrounding pixels of the central pixel of 3 × 3 are examined to find out the ridge ending. Finally the following genuine cases as shown in Figure 3.11 are considered as ridge ending conditions.

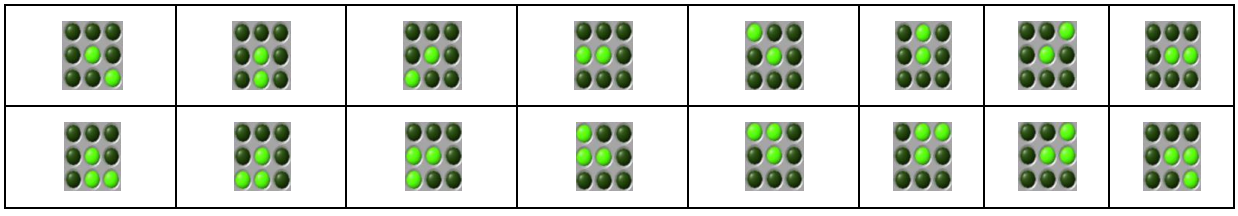


Figure 3.11 Conditions for ridge ending

The Truth table and the corresponding Hex values of the ridge ending conditions are shown in Table 3.6.

Table 3.6 Truth table of ridge ending

P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	Hex. Value
0	0	0	0	0	0	0	1	01
0	0	0	0	0	0	1	0	02
0	0	0	0	0	1	0	0	04
0	0	0	0	1	0	0	0	08
0	0	0	1	0	0	0	0	10
0	0	1	0	0	0	0	0	20
0	1	0	0	0	0	0	0	40
1	0	0	0	0	0	0	1	81
0	0	0	0	0	0	1	1	03
0	0	0	0	0	1	1	0	06
0	0	0	0	1	1	0	0	0C
0	0	0	1	1	0	0	0	18
0	0	1	1	0	0	0	0	30
0	1	1	0	0	0	0	0	60
1	1	0	0	0	0	0	0	C0
1	0	0	0	0	0	0	0	80

From the truth table given in Table 3.6, a pixel in an image is a ridge ending if {(Sum of 3×3 window is 2) + [(Sum of 3×3 window is equal to 3) & {(P_1& P_2) + (P_2&P_3) + (P_3&P_4) + (P_4&P_5) + (P_5&P_6) + (P_6&P_7) + (P_7&P_8) + (P_1&P_8)}]}= 1

There are total 16 genuine ridge ending conditions as shown in Table 3.6. The minimized logical expression solved by K map of all these 16 conditions is given by the following logical expression

(~P_1&&~ P_2&&~ P_3&& P_5&&~ P_6&&~ P_7&&~ P_8)||(~ P_1&&~ P_2&&~ P_3&&~ P_4 && P_6&&~ P_7&&~ P_8)||(~ P_1&&~ P_2&&~ P_3&&~ P_4&&~ P_5&& P_7&&~ P_8)||(~ P_1&&~ P_2&&~ P_3&&~ P_4&&~ P_5&&~ P_6&& P_8)||(P_1&&~ P_2&&~ P_3&&~ P_4&&~ P_5&&~ P_6&&~ P_7)||(P_2&&~ P_3&&~ P_4&&~ P_5&&~ P_6&&~ P_7&&~ P_8)||(~ P_1&& P_3&&~ P_4&&~ P_5&&~ P_6&&~ P_7&&~ P_8)||(~ P_1&&~ P_2&& P_4&&~ P_5&&~ P_6&&~ P_7&&~ P_8)
Where:
~ stands for Logical NOT operation

+ stands for logical OR operation

& stands for logical AND operation

|| stands for Short circuit logical OR operation

&& stands for Short circuit logical AND operation

3.2.1.2 Ridge Bifurcation

Ridge Bifurcation is the point where the ridge splits from the single line to two lines. e.g. for window of Figure 3.1 if, pixel values are $P_1 = 0$, $P_2 = 1$, $P_3 = 0$, $P_4 = 1$, $P_5 = 0$, $P_6 = 1$, $P_7 = 0$, $P_8 = 0$ then the resulted ridge bifurcation is shown in Figure 3.12.

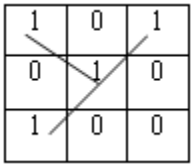
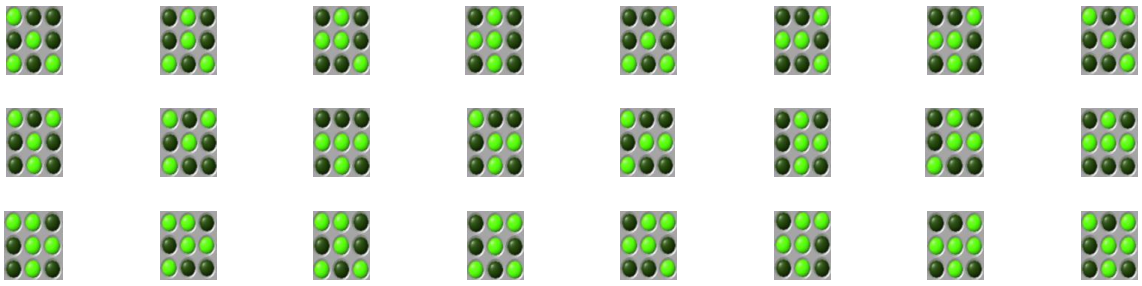


Figure 3.12 Ridge bifurcation example

All 256 cases of different combinations of the eight neighboring pixels are examined and the genuine cases are given in Figure 3.13.



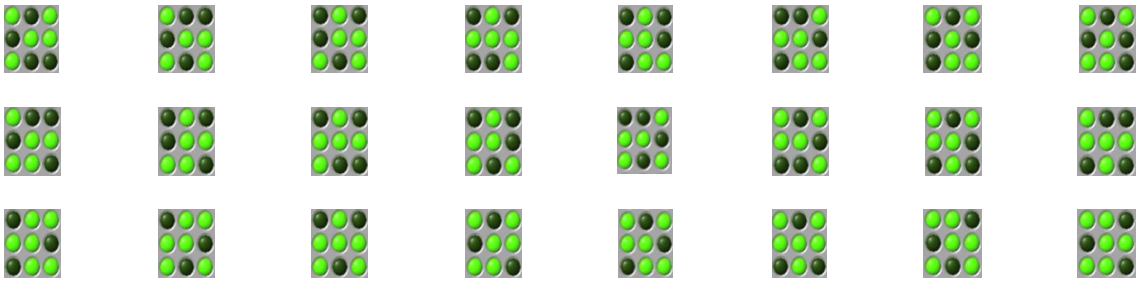


Figure 3.13 Conditions for ridge bifurcation

The Truth table and the corresponding Hex values of the ridge ending conditions are shown in Table 3.7.

Table 3.7 Truth table of ridge bifurcation

P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	Hex. Value
0	0	0	1	0	1	0	1	15
0	0	1	0	0	1	0	1	25
0	0	1	0	1	0	0	1	29
0	0	1	0	1	0	1	0	2A
0	1	0	0	0	1	0	1	45
0	1	0	0	1	0	0	1	49
0	1	0	0	1	0	1	0	4A
0	1	0	1	0	0	0	1	51
0	1	0	1	0	0	1	0	52
0	1	0	1	0	1	0	0	54
1	0	0	0	1	0	1	0	8A
1	0	0	1	0	0	1	0	92
1	0	0	1	0	1	0	0	94
1	0	1	0	0	0	1	0	A2
1	0	1	0	0	1	0	0	A4
1	0	1	0	1	0	0	0	A8
1	0	1	1	0	0	1	0	B2
1	0	1	1	0	1	0	0	B4
0	0	1	1	0	1	0	1	35
0	1	1	0	0	1	0	1	65
0	1	1	0	1	0	0	1	69
0	1	1	0	1	0	1	0	6A
1	1	0	0	1	0	1	0	CA
1	1	0	1	0	0	1	0	D2
1	1	0	1	0	1	0	0	D4
1	0	0	1	0	1	0	1	95
1	0	1	0	0	1	0	1	A5
1	0	1	0	1	0	0	1	A9

0	0	1	0	1	0	1	1	2B
0	1	0	0	1	0	1	1	4B
0	1	0	1	0	0	1	1	53
0	1	0	1	0	1	1	0	56
1	0	0	1	0	1	1	0	96
1	0	1	0	0	1	1	0	A6
1	0	1	0	1	1	0	0	AC
0	0	1	0	1	1	0	1	2D
0	1	0	0	1	1	0	1	4D
0	1	0	1	1	0	0	1	59
0	1	0	1	1	0	1	0	5A
1	0	0	1	1	0	1	0	9A
0	1	1	0	1	0	1	1	6b
0	1	1	0	1	1	0	1	6D
1	0	1	0	1	1	0	1	AD
1	1	0	1	0	1	1	0	D6
0	1	0	1	1	0	1	1	5B
1	1	0	1	1	0	1	0	DA
1	0	1	1	0	1	0	1	B5
1	0	1	1	0	1	1	0	B6

From the truth table given in Table 2, a pixel in an image is a ridge bifurcation if (Sum of 3 $\times$ 3 window is either 4 or 5 or 6) & (Any of the condition shown in Table 2) =1

In all, 48 such cases are formed for ridge bifurcation as given in Table 3.7. The minimized logical expression solved by K map of all 48 bifurcation conditions is given by the following expression

$(\sim P_1\&\&P_2\&\&\sim P_4\&\&P_5\&\&\sim P_6\&\&P_8)||(P_2\&\&\sim P_3\&\&P_5\&\&\sim P_6\&\&P_7\&\&\sim P_8)||(\sim P_1\&\&P_3\&\&\sim P_4\&\&P_5\&\&\sim P_6\&\&P_7)||(P_1\&\&\sim P_2\&\&P_3\&\&\sim P_4\&\&P_6\&\&\sim P_7)||(\sim P_1\&\&P_2\&\&\sim P_4\&\&P_6\&\&\sim P_7\&\&P_8)||(\sim P_1\&\&P_3\&\&\sim P_4\&\&P_6\&\&\sim P_7\&\&P_8)||(\sim P_2\&\&P_4\&\&\sim P_5\&\&P_6\&\&\sim P_7\&\&P_8)||(P_1\&\&\sim P_2\&\&P_4\&\&\sim P_5\&\&P_6\&\&\sim P_8)||(P_2\&\&\sim P_3\&\&P_4\&\&\sim P_5\&\&P_6\&\&\sim P_8)||(P_1\&\&\sim P_2\&\&P_4\&\&\sim P_5\&\&P_7\&\&\sim P_8)||(P_1\&\&\sim P_2\&\&P_3\&\&\sim P_5\&\&P_7\&\&\sim P_8)||(P_2\&\&\sim P_3\&\&P_4\&\&\sim P_5\&\&P_7\&\&\sim P_8)||(\sim P_1\&\&P_2\&\&\sim P_3\&\&P_4\&\&\sim P_6\&\&P_8)||(P_1\&\&\sim P_2\&\&P_3\&\&\sim P_4\&\&P_5\&\&\sim P_6\&\&\sim P_7)||(\sim P_2\&\&P_3\&\&\sim P_4\&\&P_5\&\&\sim P_6\&\&\sim P_7\&\&P_8)||(P_1\&\&\sim P_2\&\&\sim P_3\&\&P_5\&\&\sim P_6\&\&P_7\&\&\sim P_8)$

All the conditions given in Table 3.6 and Table 3.7 are solved using the K map to obtain the combined minimized logical expression. The resulting K map is shown in Figure 3.14.

	0000	0001	0011	0010	0110	0111	0101	0100	1100	1101	1111	1110	1010	1011	1001	1000
0000	0	1	1	1	1	0	0	1	1	0	0	0	0	0	0	1
0001	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1
0011	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0
0010	1	0	0	0	0	0	1	0	0	1	0	0	1	1	1	0
0110	0	0	1	0	0	1	0	0	0	0	0	0	0	1	1	1
0111	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0101	1	1	0	1	0	1	0	1	0	0	0	1	0	0	1	1
0100	0	0	1	0	0	1	0	0	0	0	1	0	0	1	1	1
1100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
1101	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	1
1111	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1110	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1010	0	0	0	1	1	0	1	1	1	1	0	0	0	0	1	1
1011	0	0	0	1	1	0	1	1	0	0	0	1	0	0	0	0
1001	0	0	0	1	1	0	1	1	0	0	0	0	1	0	0	0
1000	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0

Figure 3.14 K map of Combined Minutiae Extraction Rules

The combined minimized logical expression for minutiae (ridge ending and bifurcation) extraction is given by

$X=(P_2\&\&\sim P_3\&\&P_5\&\&\sim P_6\&\&\sim P_7\&\&\sim P_8)||(\sim P_1\&\&P_2\&\&\sim P_4\&\&P_5\&\&\sim P_6\&\&\sim P_7)||(\sim P_2\&\&P_3\&\&\sim P_4\&\&P_6\&\&\sim P_7\&\&P_8)||(\sim P_2\&\&P_4\&\&\sim P_5\&\&P_6\&\&\sim P_7\&\&P_8)||(P_1\&\&\sim P_2\&\&P_4\&\&\sim P_5\&\&P_6\&\&\sim P_8)||(P_1\&\&\sim P_2\&\&P_3\&\&\sim P_5\&\&P_6\&\&\sim P_8)||(P_1\&\&\sim P_2\&\&P_3\&\&\sim P_5\&\&P_7\&\&\sim P_8)||(\sim P_1\&\&P_2\&\&\sim P_4\&\&\sim P_6\&\&P_7\&\&P_8)||(P_2\&\&\sim P_3\&\&P_4\&\&\sim P_5\&\&\sim P_7\&\&\sim P_8)||(P_2\&\&\sim P_3\&\&P_4\&\&\sim P_5\&\&\sim P_6\&\&\sim P_8)||(\sim P_1\&\&P_2\&\&\sim P_3\&\&P_4\&\&\sim P_6\&\&\sim P_7)||(\sim P_2\&\&P_3\&\&\sim P_4\&\&P_5\&\&\sim P_6\&\&\sim P_7\&\&P_8)||(P_1\&\&\sim P_2\&\&\sim P_3\&\&P_5\&\&\sim P_6\&\&P_7\&\&\sim P_8)||(\sim P_1\&\&\sim P_2\&\&P_3\&\&\sim P_4\&\&P_5\&\&\sim P_6\&\&P_7)||(\sim P_2\&\&P_3\&\&P_4\&\&P_5\&\&P_6\&\&P_7\&\&\sim P_8)||(P_1\&\&\sim P_2\&\&P_3\&\&\sim P_4\&\&P_5\&\&\sim P_7\&\&\sim P_8)||(\sim P_1\&\&\sim P_2\&\&\sim P_3\&\&\sim P_4\&\&P_5\&\&\sim P_7\&\&\sim P_8)||(\sim P_1\&\&P_2\&\&\sim P_3\&\&\sim P_4\&\&P_6\&\&P_7\&\&P_8)||(\sim P_1\&\&P_2\&\&\sim P_3\&\&\sim P_5\&\&P_6\&\&P_7\&\&P_8)||(\sim P_1\&\&P_2\&\&\sim P_4\&\&\sim P_5\&\&P_6\&\&P_7\&\&P_8)||(\sim P_1\&\&\sim P_2\&\&\sim P_3\&\&\sim P_4\&\&\sim P_5\&\&P_6\&\&\sim P_8)||(P_1\&\&\sim P_2\&\&\sim P_3\&\&P_4\&\&\sim P_6\&\&P_7\&\&\sim P_8)||(\sim P_1\&\&\sim P_2\&\&\sim P_3\&\&\sim P_4\&\&\sim P_5\&\&\sim P_6\&\&P_7)||(\sim P_1\&\&\sim P_2\&\&\sim P_3\&\&\sim P_4\&\&\sim P_5\&\&\sim P_6\&\&P_8)||(P_1\&\&\sim P_2\&\&\sim P_3\&\&\sim P_4\&\&\sim P_5\&\&\sim P_6\&\&\sim P_7)||(\sim$

P_1&&~P_2&&P_3&&~P_5&&~P_6&&~P_7&&~P_8)||(~P_1&&~P_2&&~P_3&&P_4&&~P_6&&~P_7&&~P_8)||(~P_1&&P_2&&~P_3&&P_4&&P_5&&P_6&&P_7&&~P_8);

If X = $\begin{cases} 1 & P \text{ is a Minutiae Point} \\ 0 & \text{Not a Minutiae Point} \end{cases}$

Where, P is the pixel in question.

3.2.2 Difference in Proposed Method and Crossing Number Method

The proposed method is different from the CN method in the following ways:

- The minutiae owing to the spike structure are eliminated, because for a spike to occur, one of the conditions shown in Figure 3.15 must be present i.e.

  [(P_1 && P_2 && P_8) || (P_2 && P_3 && P_4) || (P_4 && P_5 && P_6) || (P_6 && P_7 && P_8)] = 1

  For crossing number method these are ridge ending conditions but in the proposed method these conditions are eliminated.

Figure 3.15 Conditions for spike

- In a 3 × 3 window, if up to four consecutive pixels are zero ridge ending conditions may not occur in actual (The conditions may occur due to improper thinning), as shown in Figure 3.16 but crossing number method consider these conditions as ridge endings. All these conditions are also eliminated by the proposed method.

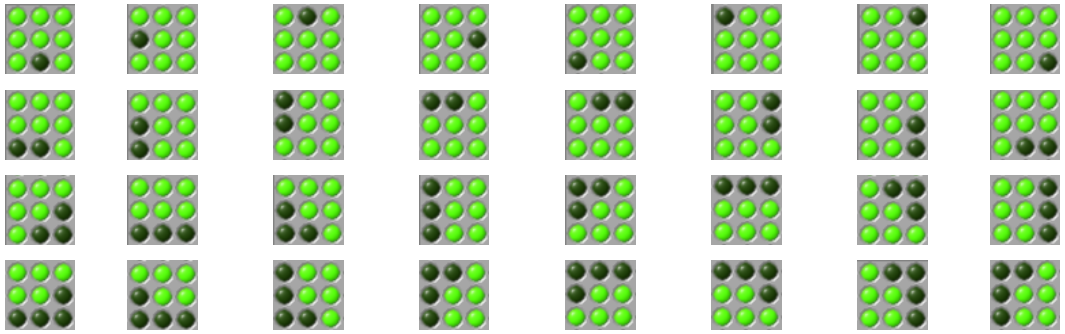


Figure 3.16 False ridge ending conditions considered by CN method

- The false ridge bifurcation conditions shown in Figure 3.17 are also eliminated by the proposed method, which are considered as bifurcations by CN method.

Figure 3.17 False ridge bifurcation conditions considered by CN method

- Few false minutiae are identified as a result of border because the image ends abruptly at the border so additionally following rules have been incorporated in the proposed algorithm to remove the false border minutiae.
  - (i) Sum all the values in the row towards the right of the pixel in question
  - (ii) Sum all the values in the row towards the left of the pixel in question
  - (iii) Sum all the values in the column on the top of the pixel in question
  - (iv) Sum all the values in the column below the pixel in question

  If sum of the values either of the above steps is zero then the minutiae is due to border and ignore it. Owing to these reasons the proposed method gives better results as compared to CN method.

3.2.3 Results, Comparison and Discussions of Minutiae Extraction Algorithm

A new feature (minutiae) extraction algorithm using minimum logical expression has been discussed. The experiments conducted on the FVC2002/Db1_a database and comparison of crossing number and proposed method in Table 3.8 and Table 3.9 shows that the proposed method of minutiae extraction is far better than the crossing number method. Table 3.8 shows the comparison of minutiae extracted by crossing number and proposed method without removing the border minutiae, while Table 3.9 gives the comparison of the extracted minutiae by the two methods when minutiae due to border are also removed by the proposed method. Table 3.8 also shows the coordinates (considering the coordinates of top left corner pixel as {1, 1}) of the false ridge bifurcation points eliminated by the proposed method. Comparison of two methods reflects that the proposed method eliminates most of false minutiae in the extraction stage which remains with the crossing number method.

Table 3.8 Comparison of proposed method (without removing border minutiae) and CN method

Sr. no.	Image	CN method		Proposed		Difference		Pixels coordinates(X/Y) where false bifurcation are detected
		Ending	Bifur	Ending	Bifur	Ending	Bifur	
1	1_1	344	85	227	85	117	0	
2	2_1	403	106	303	105	100	1	(1/224)
3	3_1	590	190	405	184	185	6	(1/174),(303/199),(323/279), (337/280),(359/243),(361/270)
4	4_1	355	86	229	85	126	1	(71/193)
5	5_1	320	99	215	99	105	0	
6	6_1	219	215	149	210	70	5	(111/237),(135/265),(191/269), (366/118),(366/197)
7	7_1	369	80	257	78	112	2	(63/280), (366/54)
8	8_1	347	293	235	290	112	3	(362/308), (366/207), (366/129)
9	9_1	207	75	178	75	29	0	
10	10_1	440	104	326	104	114	0	
11	11_1	353	36	304	34	49	2	(158/310),(172/316)
12	12_1	470	71	396	71	74	0	
13	13_1	412	120	334	120	78	0	
14	14_1	784	103	722	103	62	0	
15	15_1	402	129	289	129	113	0	
16	16_1	928	336	811	331	117	5	(47/295), (143/176), (169/244), (185/319), (239/232)
17	17_1	415	173	330	172	85	1	(87/162)
18	18_1	476	71	400	71	76	0	
19	19_1	417	193	318	192	99	1	(168/81)
20	20_1	681	36	640	35	41	1	(159/240)
21	21_1	322	320	206	319	116	1	(295/103)
22	22_1	352	336	237	333	115	3	(52,222), (217/112), (351/284)
23	23_1	625	106	517	105	108	1	(87/272)
24	24_1	418	88	317	87	101	1	(366/277)
25	25_1	401	93	328	93	73	0	
26	26_1	262	170	165	169	97	1	(88/299)
27	27_1	418	56	388	56	30	0	
28	28_1	308	39	228	39	80	0	
29	29_1	492	78	436	78	56	0	
30	30_1	472	69	393	67	79	2	(18/240), (223/280)
31	31_1	609	65	528	65	81	0	
32	32_1	458	58	418	58	40	0	
33	33_1	388	36	304	36	84	0	
34	34_1	389	108	249	107	140	1	(1/127)
35	35_1	402	85	298	85	104	0	
36	36_1	379	336	299	333	80	3	(160/308), (255/137),

								(366/244)
37	37_1	252	114	168	113	84	1	(122/292)
38	38_1	804	255	690	252	114	3	(1/155), (1/215), (186/269)
39	39_1	380	133	288	133	92	0	
40	40_1	462	38	416	38	46	0	

Table 3.9 Comparison of proposed method (after removing border minutiae) and CN method

Sr. no.	Image	CN method		Proposed		Difference		Total difference	%age difference
		Ending	Bifur	Ending	Bifur	Ending	Bifur		
1	1_1	344	85	132	85	212	0	212	97.7
2	2_1	403	106	138	105	265	1	266	109.5
3	3_1	590	190	144	184	446	6	452	137.8
4	4_1	355	86	84	85	271	1	272	160.9
5	5_1	320	99	106	99	214	0	214	104.4
6	6_1	219	215	75	210	144	5	149	52.3
7	7_1	369	80	87	78	282	2	284	172.1
8	8_1	347	293	147	290	200	3	203	46.5
9	9_1	207	75	127	75	80	0	80	39.6
10	10_1	440	104	161	104	279	0	279	105.3
11	11_1	353	36	177	34	176	2	178	84.4
12	12_1	470	71	175	71	295	0	295	119.9
13	13_1	412	120	190	120	222	0	222	71.6
14	14_1	784	103	483	103	301	0	301	51.4
15	15_1	402	129	160	129	242	0	242	83.7
16	16_1	928	336	522	331	406	5	411	48.2
17	17_1	415	173	181	172	234	1	235	66.6
18	18_1	476	71	208	71	268	0	268	96.1
19	19_1	417	193	144	192	273	1	274	81.5
20	20_1	681	36	408	35	273	1	274	61.9
21	21_1	322	320	134	319	188	1	189	41.7
22	22_1	352	336	109	333	243	3	246	55.7
23	23_1	625	106	284	105	341	1	342	87.9
24	24_1	418	88	204	87	214	1	215	73.9
25	25_1	401	93	107	93	294	0	294	147.0
26	26_1	262	170	52	169	210	1	211	95.5
27	27_1	418	56	184	56	234	0	234	97.5
28	28_1	308	39	117	39	191	0	191	122.4
29	29_1	492	78	261	78	231	0	231	68.1
30	30_1	472	69	221	67	251	2	253	87.8

31	31_1	609	65	345	65	264	0	264	64.4
32	32_1	458	58	173	58	285	0	285	123.4
33	33_1	388	36	224	36	164	0	164	63.1
34	34_1	389	108	108	107	281	1	282	131.2
35	35_1	402	85	175	85	227	0	227	87.3
36	36_1	379	336	142	333	237	3	240	50.5
37	37_1	252	114	61	113	191	1	192	110.3
38	38_1	804	255	485	252	319	3	322	43.7
39	39_1	380	133	146	133	234	0	234	83.9
40	40_1	462	38	362	38	100	0	100	25.0

The percentage difference in the above table represents the error (false minutiae) and is calculated as

$$\frac{Minutiae\,calculated\,by\,CN\,method - Minutiae\,calculated\,by\,proposed\,method}{Minutiae\,calculated\,by\,proposed\,method} \times 100$$

The Figure 3.18 is a graphical representation of total number of minutiae extracted by the CN method and the proposed method. It can be easily concluded from the graph that the proposed method eliminate most of the false minutiae (including the border minutiae) which are left with the CN method.

The expanded portions of thinned fingerprint images from FVC 2002/Db1_a database are shown in Figure 3.19 and Figure 3.20 of ridge ending and ridge bifurcation respectively, in which the marked 3×3 windows shows some of false minutiae points, to which the CN method counts as valid minutiae (ridge endings or bifurcations) points. These points need to be eliminated in the post processing stage while in the proposed algorithm these points are automatically eliminated.

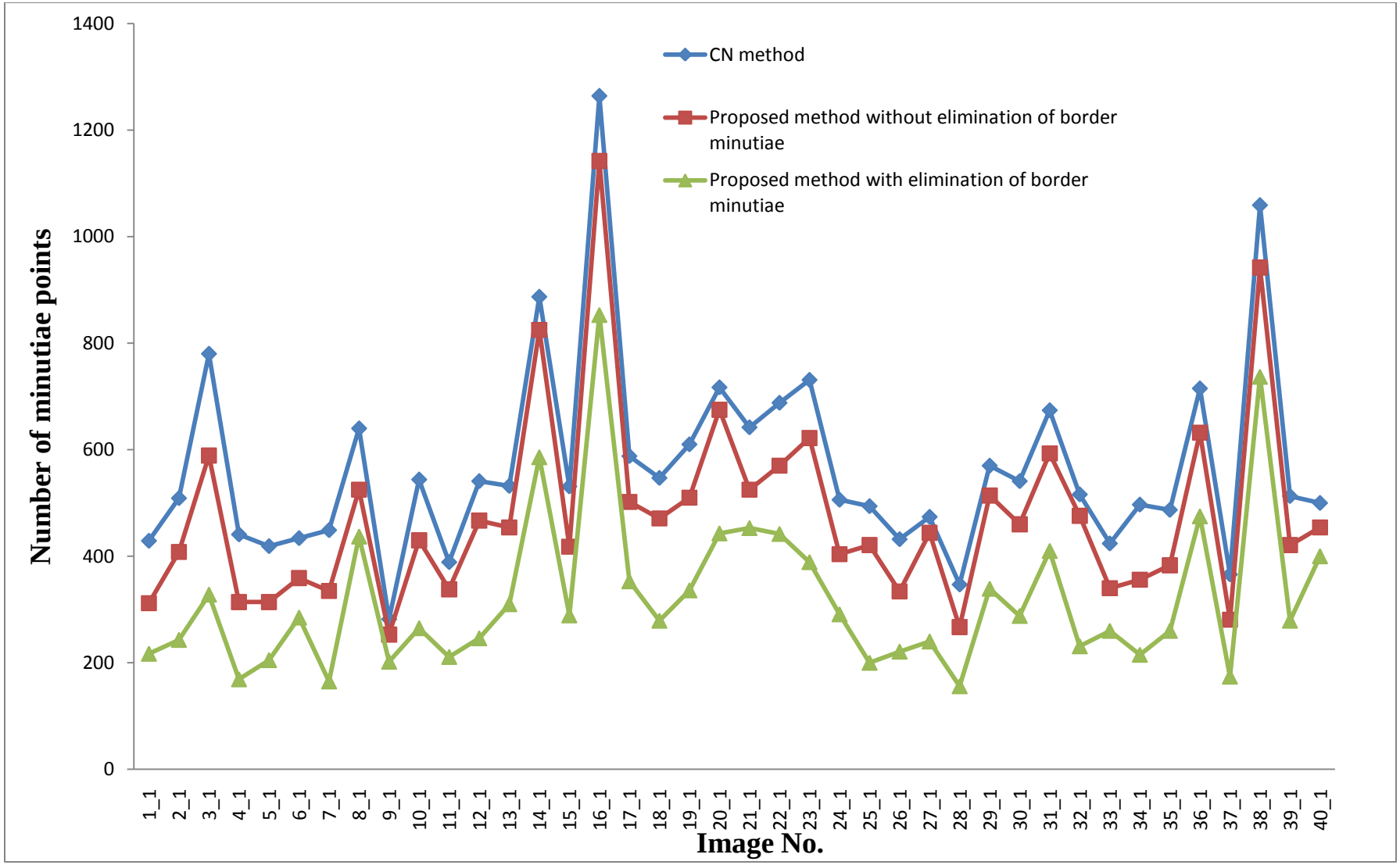
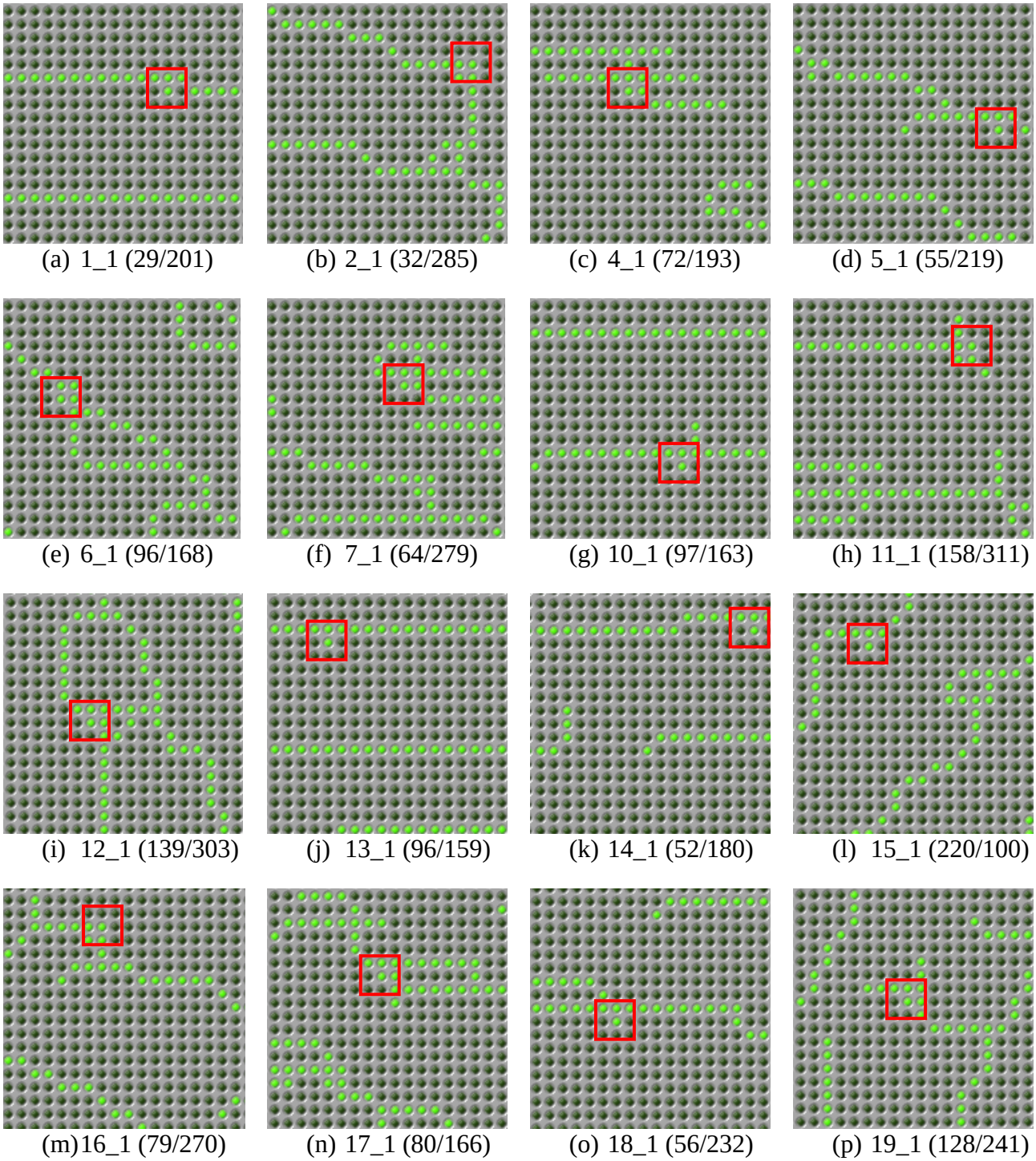


Figure 3.18 Comparison of CN method and proposed method (with and without border pixel elimination)



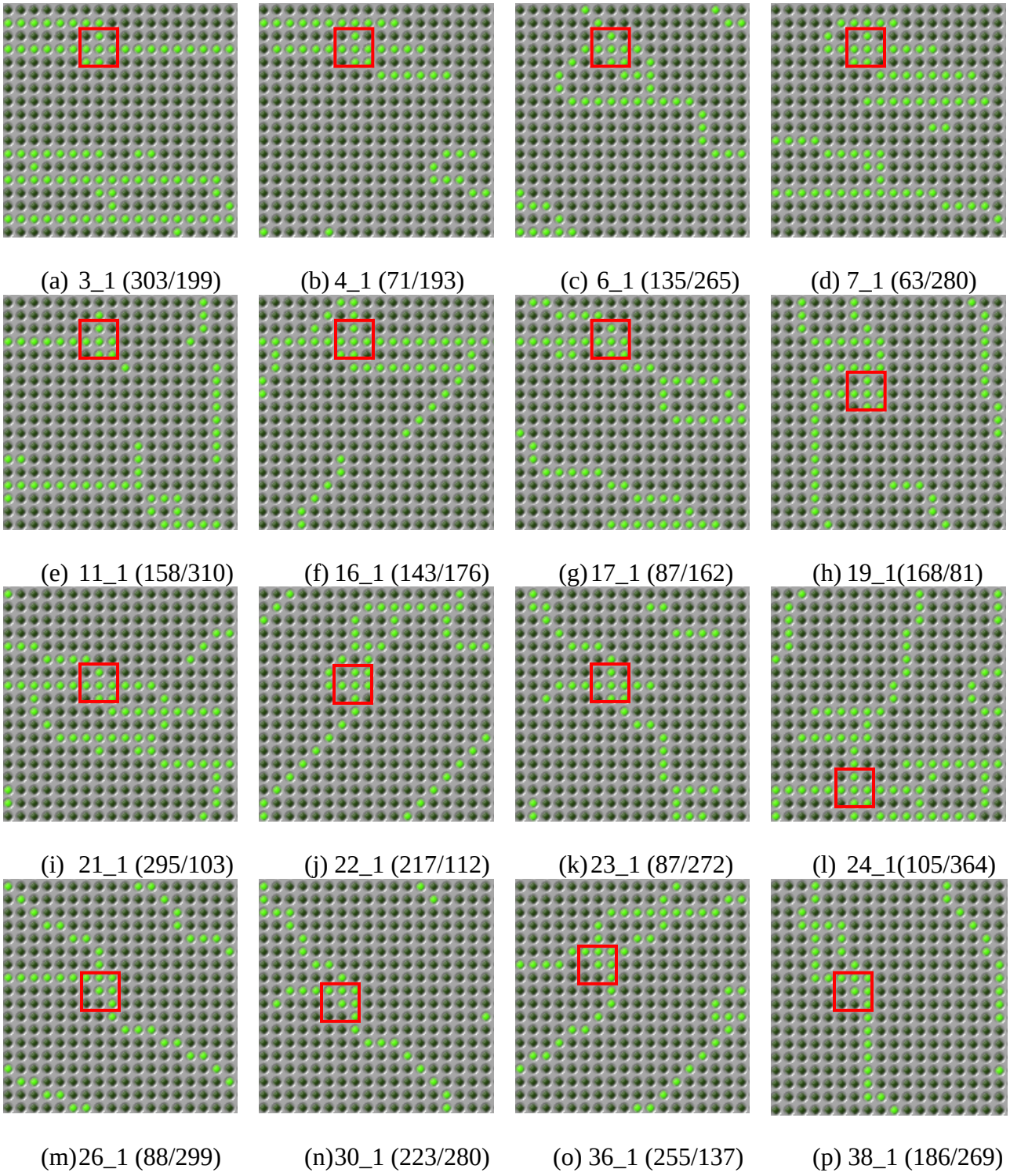
(a) 1_1 (29/201) (b) 2_1 (32/285) (c) 4_1 (72/193) (d) 5_1 (55/219)

(e) 6_1 (96/168) (f) 7_1 (64/279) (g) 10_1 (97/163) (h) 11_1 (158/311)

(i) 12_1 (139/303) (j) 13_1 (96/159) (k) 14_1 (52/180) (l) 15_1 (220/100)

(m) 16_1 (79/270) (n) 17_1 (80/166) (o) 18_1 (56/232) (p) 19_1 (128/241)

Figure 3.19 Expanded versions of the different parts of the thinned images. Rectangular window shows the false ridge ending minutiae rejected by proposed algorithm. (Caption shows FVC 2002/Db1_a database fig. no. followed by coordinates (x/y) of the pixel in question)



(a) 3_1 (303/199) (b) 4_1 (71/193) (c) 6_1 (135/265) (d) 7_1 (63/280)

(e) 11_1 (158/310) (f) 16_1 (143/176) (g) 17_1 (87/162) (h) 19_1(168/81)

(i) 21_1 (295/103) (j) 22_1 (217/112) (k) 23_1 (87/272) (l) 24_1(105/364)

(m) 26_1 (88/299) (n) 30_1 (223/280) (o) 36_1 (255/137) (p) 38_1 (186/269)

Figure 3.20 Expanded versions of the different parts of the thinned images. Rectangular window shows the false ridge bifurcations minutiae rejected by proposed algorithm. (Caption shows FVC 2002/Db1_a database fig. no. followed by coordinates (x/y) of the pixel in question)

3.3 Post Processing

Most of the false minutiae points including spike points are eliminated in the proposed minutiae extraction algorithm. Still, there may exist some false minutiae points which are required to be eliminated. False minutiae are introduced into the image due to factors such as noisy images and image artifacts created by the thinning process. Figure 3.21 illustrates some examples of false minutiae structures, which include the spur, hole, triangle and spike structures [164].

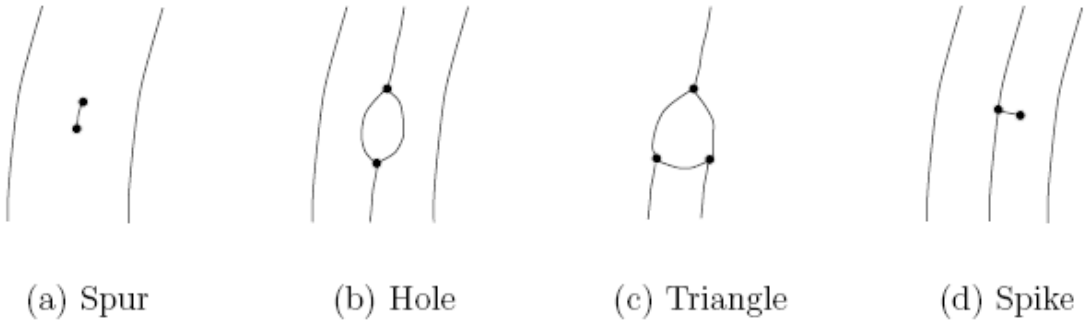


Figure 3.21 Some of typical false minutiae structures [164]

The problems of fingerprint image post processing for false minutiae elimination have been addressed by different authors in a different manner. Xiao and Raafat [164] introduced an ad hoc approach to remove false minutiae structures. They proposed a rule based algorithm which requires some numerical characteristics associated with the minutiae such as length of ridge(s), the minutia angle, and the number of facing minutiae in a neighborhood. Hung [165] proposed a set of algorithms using the property of duality between the ridge and valley structures for detecting and removing spurs, holes and bridges. Hung's algorithm uses thinned images and only ridge minutiae having a counterpart (of complementary type) in the valley skeleton are retained. In Ratha et al. [80] algorithm validation of minutiae is based on a set of three heuristic rules. For example, a ridge ending point that is connected to a bifurcation point, and is below a certain threshold distance is eliminated. This heuristic rule corresponds to removal of the spike structure. Additional heuristic rules are then used to eliminate other types of false minutiae. Furthermore, a boundary effect treatment is applied where the minutiae below a certain distance from the boundary of the foreground region are

deleted. A novel approach to the validation of minutiae is the post processing algorithm proposed by Tico and Kuosmanen [166]. This algorithm operates on the skeleton image. This approach incorporates the validation of different types of minutiae into a single algorithm. It tests the validity of each minutiae point by scanning the skeleton image and examining the local neighborhood around the minutiae. The algorithm is then able to cancel out false minutiae based on the configuration of the ridge pixels connected to the minutiae point. A Tariq et al. [167] proposed a windowing method of post processing which takes into account the minutiae neighboring information in a fingerprint image to validate ridge ending and bifurcations. They used separate elimination and validation rules for ridge ending and bifurcation. In the present work the windowing method has been used but instead of validating the minutiae separately, the same rules for bifurcation and ending have been used.

3.3.1 Post Processing Algorithm

The algorithm of post processing used in this work is as:

1. Select the window size
2. Extract the minutiae point in question obtained from 3 x 3 window
3. Store 1 or 3 i.e. type of minutiae (1 for ridge ending and 3 for ridge bifurcation) in the variable flag.
4. Increase the size of the window around the pixel in question by 2 i.e. from 3x3 to 5x5 or from 5x5 to 7x7 and so on.
5. Extract the pixels which are connected to the central pixel and make all the other pixels zero
6. Check the 0 to 1 transitions of the boundary pixels for the extracted window
7. Store the result in flag
8. Repeat the steps 4 to 7 up to window size
9. If all the values in a flag are same then it is a valid minutiae point and stores its content (x, y, θ and type).
10. Repeat the steps 2 to 9 for all the minutiae points extracted during feature extraction stage.

Experiments have been conducted on different fingerprint images and for different window sizes by applying the above algorithm. The effect of the window sizes on the minutiae validation is as shown in Figure 3.22, Figure 3.23 and Figure 3.24 for image 1_1, 2_1 and 4_1 respectively of FVC2002/Db1_a database. The red dots in the images of Figure 3.22, Figure 3.23 and Figure 3.24 represents the minutiae points where as the blue circles represent some of the false minutiae points and green circles shows some of the lost (genuine) minutiae points.

From the experimental results it has been observed that as the value of window size increases total number of minutiae points go on decreasing. At the small window size the number of false minutiae points are more and false minutiae go on decreasing as window size has been increased. If the window size has been further increased some genuine minutiae points may also be lost which will affect the accuracy of the system. Experimentally it has been concluded that a window size of 15 gives the optimum results.

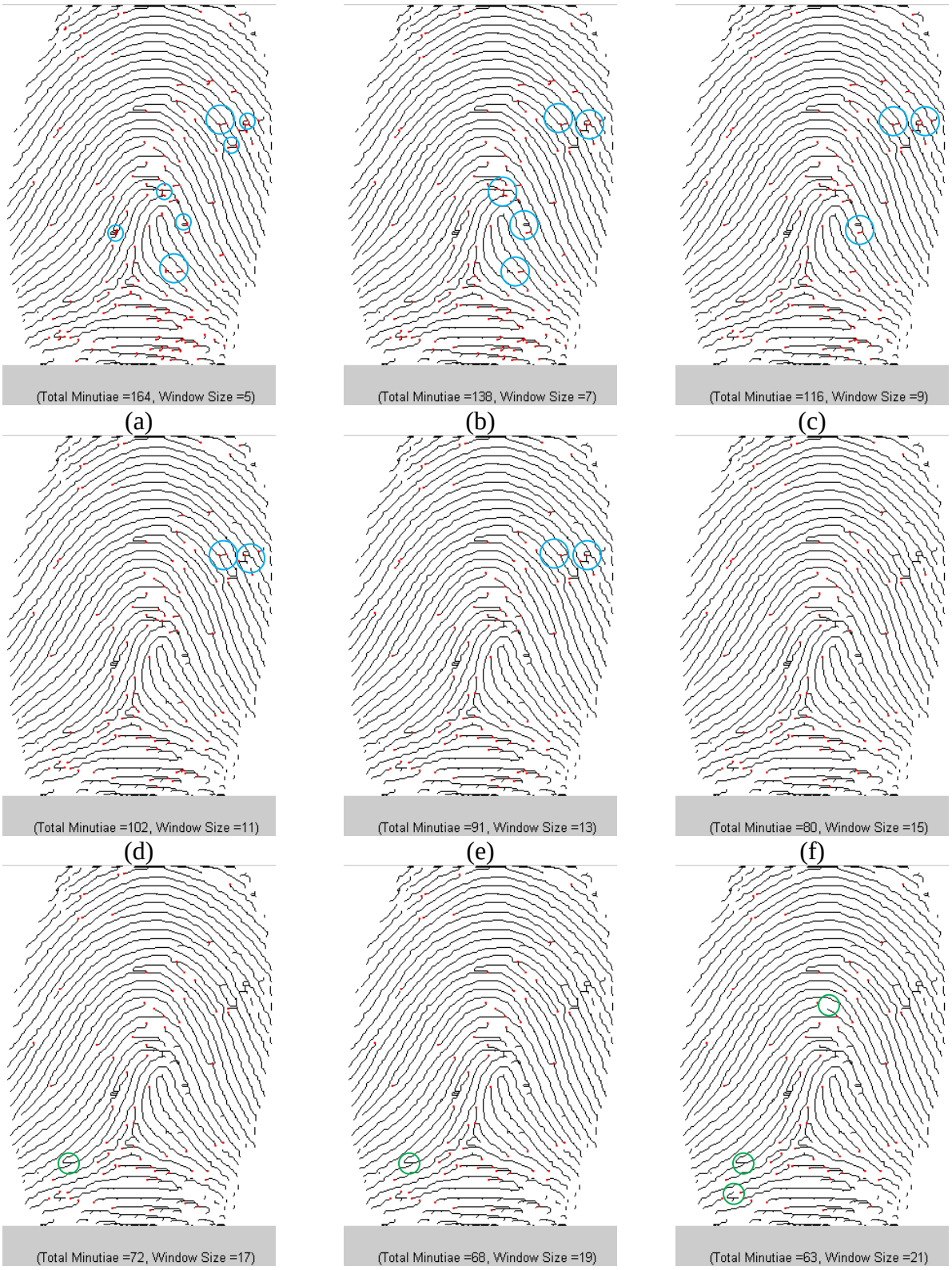


Figure 3.22 Images after post processing of image 1_1 of database FVC2002/Db1_a with different window size

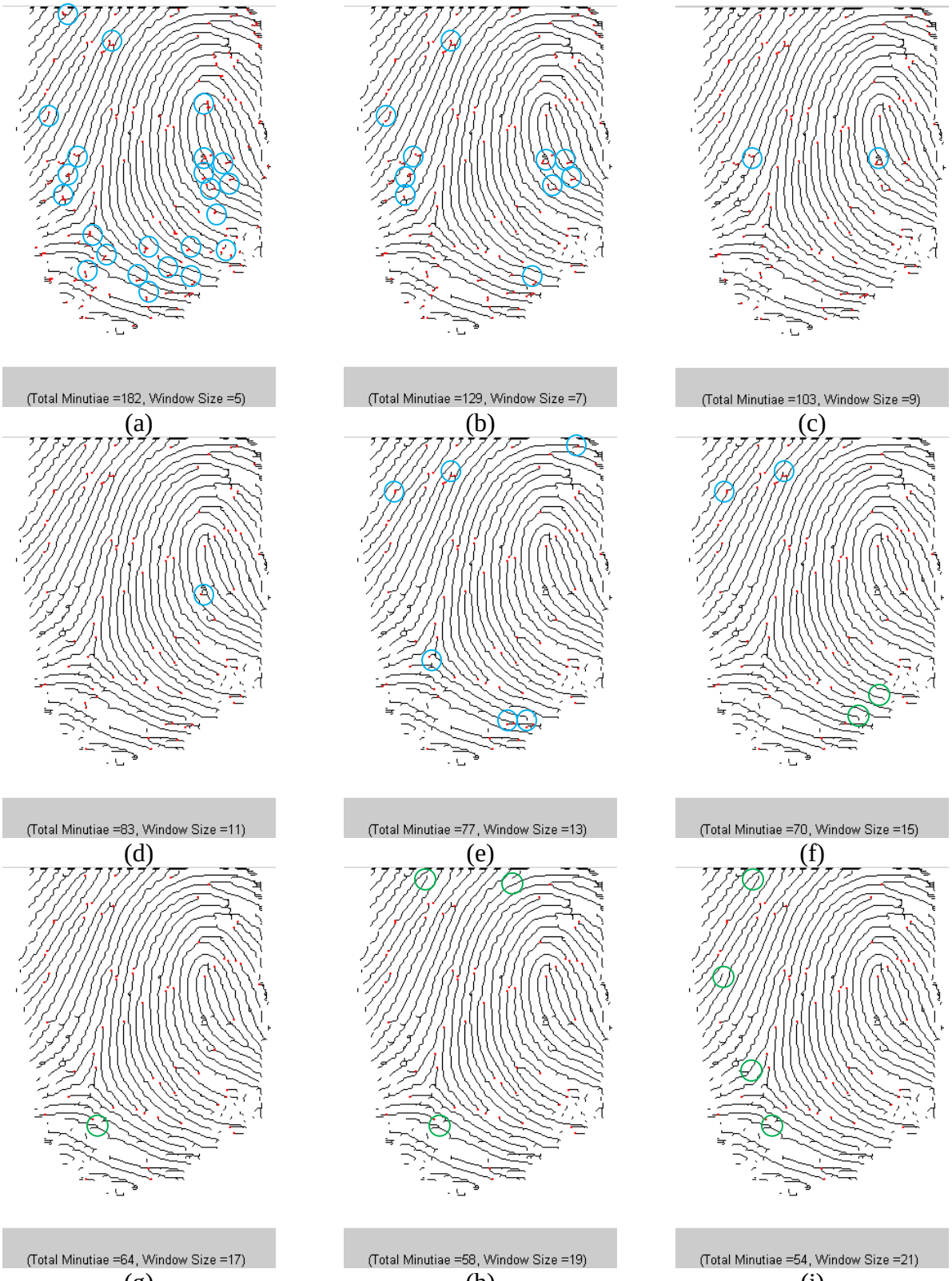
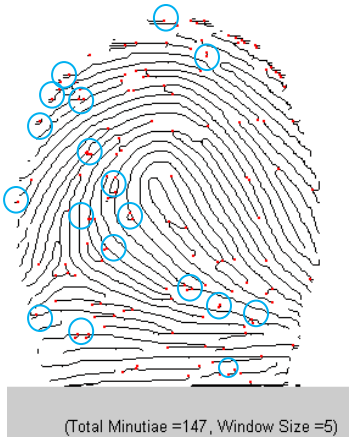
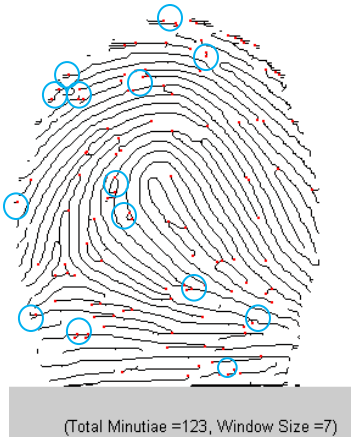


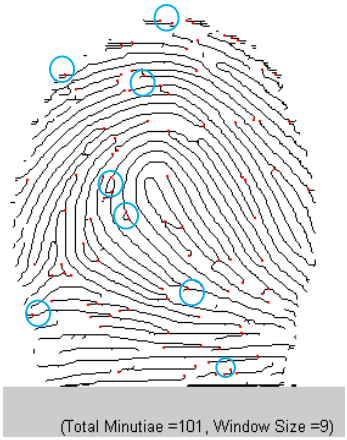
Figure 3.23 Images after post processing of image 2_1 of database FVC2002/Db1_a with different window size



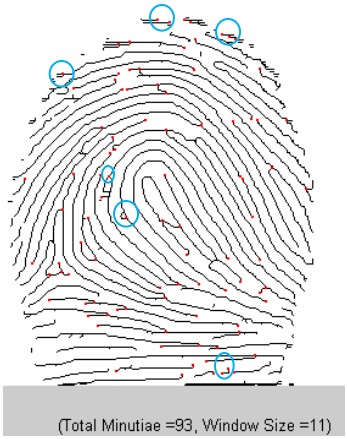
(a)



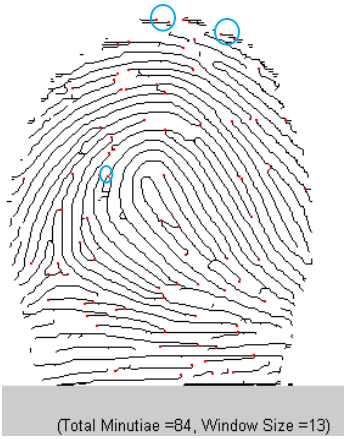
(b)



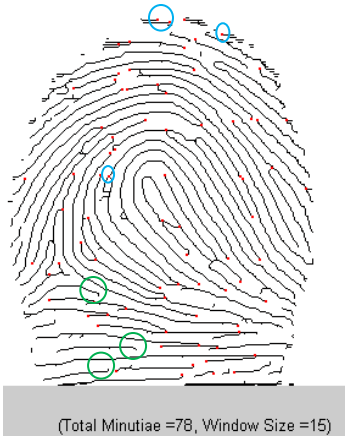
(c)



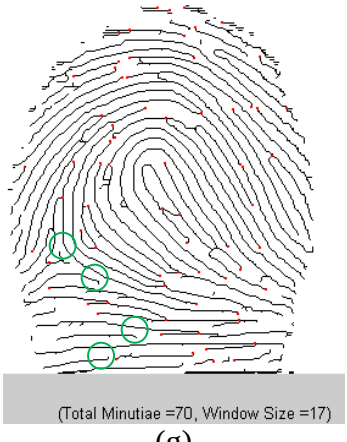
(d)



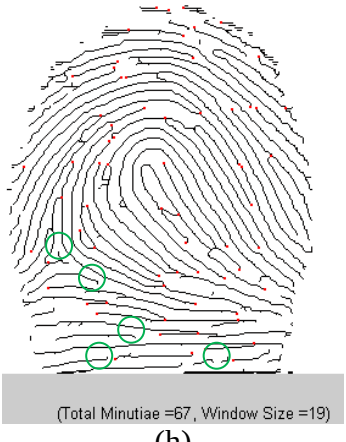
(e)



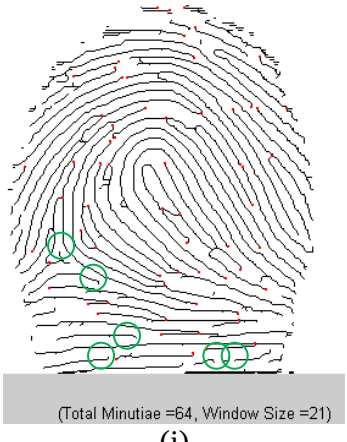
(f)



(g)



(h)



(i)

Figure 3.24 Images after post processing of image 4_1 of database FVC2002/Db1_a with different window size

3.4 Alignment and Validation

Each extracted minutiae of fingerprint image in the minutiae extraction stage is defined by its location (x, y), its orientation (θ) and its type (ridge ending or ridge bifurcation). Each minutia in the reference image is required to be matched with the corresponding minutia in the query image to find the authenticity of the person. So, the success of minutiae based fingerprint authentication systems normally depends upon the point matching algorithm. However, rotation and translation between the reference image and query image are the major issues involved for the success of an automatic fingerprint authentication system. Because, rotation and translation between the two images make it difficult to find the correspondence between the features (minutiae) of the two images.

Generally, fingerprint matching algorithm has two steps

(i) Align the template and query images.

(ii) Determine the correspondences between features of the two images.

Aligning the two fingerprints is a mandatory step in order to maximize the number of matching minutiae. Correctly aligning the fingerprints requires the translation and rotation to be recovered exactly. Different approaches of fingerprint pre-alignment divided into absolute and relative pre-alignment, proposed in the literature by the different authors and have been discussed in the chapter 2 [113-120].

In the present work, a new genetic algorithm based relative alignment method has been developed. All the three parameters x, y (translation) and θ (rotational) have been optimized separately and the fitness value is calculated using the parameters from reference and query image in the sorted form. In order to speed up the fitness evaluation function two speed enhancement steps have also been incorporated in the developed algorithm.

3.4.1 Genetic Algorithm

Genetic algorithm is a method for solving optimization problems. The genetic algorithm (GA) repeatedly modifies a population of individual solutions. At each step GA selects individuals at random from the current population to be parents and uses them to produce the children for the next generation. Over the successive generations, the population evolves towards an optimal solution [168]. The Genetic algorithm works in the following manner [169]:

1. The algorithm begins by creating a random initial population of N chromosome.
2. The algorithm then evaluates the fitness function of each member in the current population.
3. Based upon the fitness value the algorithm then creates a new population of children by using the individuals in the current population (parents). Three types of children i.e. elite children, crossover children and mutation children are created for the next generation. This process is known as reproduction and is explained in section 3.4.1.1.
4. With the newly formed generation the algorithm goes to step 2. This process is repeated until one of the stopping criteria is met.
5. The algorithm stops when one of the stopping criteria is met. The different stopping conditions are explained in the section 3.4.1.2 under the heading termination conditions.

3.4.1.1 Reproduction

Reproduction determines the creation of next generation in genetic algorithm. The various steps of reproduction are [169]

a) Elite count: It determines the number of individuals with the best fitness value in the current generation that is guaranteed to survive in the next generation. These individuals are known as elite children. The value of elite children should be small because setting the elite count to a high value means more number of fit individuals in the next generation, which will make the search less effective.

b) Crossover: The crossover children are created by combining the genes from a pairs of individuals in the current population. The crossover enables the algorithm to extract the best genes from different individuals and recombine them into potentially superior children. The crossover fraction specifies the fraction of each population, other than the elite children, that are made up of crossover children. The value of crossover fraction varies between 0 and 1. A crossover fraction of 1 means that all children other than elite children are crossover children which means the algorithm can not create any new genes. So, any value between 0 and 1 should be chosen which will give the best result.

c) Mutation: Mutation adds to the diversity of a population and thereby increases the likelihood that the algorithm will generate individuals with better fitness values. Mutation children are created by applying random changes to single individual in the current generation.

3.4.1.2 Termination Conditions

Termination conditions decide when the genetic algorithm should stop. Following are the termination conditions which may be considered for stopping the GA [169].

- **Generations**: it specifies the maximum number of iterations the genetic algorithm will perform.
- **Time Limit:** it specifies the maximum time in seconds the genetic algorithm runs before stopping.
- **Fitness Limit:** The algorithm stops if the best fitness value is less then or equal to the fitness limit.
- **Stall Generation:** If there is no improvement in the best fitness value for the number of generations indicated by the stall generation the algorithm will stop.
- **Stall Time:** If there is no improvement in the best fitness value for an interval of time in seconds indicated by the stall time the algorithm will stop.

3.4.2 Proposed Alignment Algorithm

In fingerprint authentication system main problem is due to relative displacement i.e. rotation and translation between reference and query fingerprint images. The translation is further divided into x and y directions. But $r = \sqrt{x^2 + y^2}$ can not be optimized in place of x and y because for the same change in value of x and/or y the change in value of r is different for the different base value of x and y. Thus there are three different parameters to be optimized with the help of Genetic algorithm.

Optimizing these three parameters together will pose a problem, if at some point of time an optimum value of theta is approached by the chromosome the same may not be reported as optimized value, as x and y may not be optimum at that point of time, so three being

optimum at the same time has a less probability and the answer may not be correct. In other words optimizing these three parameters separately will give an accurate result.

3.4.2.1 Fitness Evaluation Function

Fitness value is calculated by subtracting the values of reference data and value of current chromosome from the query data. Since the query data and reference data are not in order of matching so each value in the query data is compared with the all the values in the reference data and errors are calculated for each comparison. The minimum of these errors is chosen. After evaluating the errors for each value in the query data by the above modus operandi the root mean square (RMSE) of those errors is taken, which is the fitness value for the chromosome in action, likewise the fitness value for all the chromosomes of the current population is calculated

Let us take the case of theta optimization as an example, let the

Query data is : $q\theta_1, q\theta_2, q\theta_3, q\theta_4, q\theta_5, q\theta_6, q\theta_7, q\theta_8, \ldots\ldots\ldots$ ..

Reference data: $r\theta_1, r\theta_2, r\theta_3, r\theta_4, r\theta_5, r\theta_6, r\theta_7, r\theta_8, \ldots\ldots\ldots$ ..

Population generated by GA: $\theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6, \theta_7, \theta_8, \ldots\ldots\ldots$ ..

Calculate the fitness value as shown in following steps:

1. Take the first point of the population θ_1.
2. Take the first point of Query data i.e. $q\theta_1$.
3. Subtract all points of reference data and population point from the above query point and evaluate the error as:

   $E_1 = q\theta_1 - r\theta_1 - \theta_1$
   $E_2 = q\theta_1 - r\theta_2 - \theta_1$
   $E_3 = q\theta_1 - r\theta_3 - \theta_1$
   $E_4 = q\theta_1 - r\theta_4 - \theta_1$
   $E_5 = q\theta_1 - r\theta_5 - \theta_1$
   $E_6 = q\theta_1 - r\theta_6 - \theta_1$ and so on ……
4. Search out the absolute minima of errors calculated in step 3 and assign it as the error for $q\theta_1$ as qE_1, i.e. $qE_1 = \min(|E_1|, |E_2|, |E_3|, |E_4|, |E_5|, \ldots\ldots\ldots\ldots)$.
5. Repeat the steps 3 and 4 for all the points of query data.

6. Calculate the RMSE of $qE_1, qE_2, qE_3, qE_4, qE_5, \ldots\ldots\ldots$ This value of RMSE is the fitness value for θ_1.
7. Repeat the steps from 2 to 6, to calculate the fitness value for all the points in the current population.

3.4.2.2 Speed up Process

In order to reduce the computational time taken by the Genetic algorithm various speed up steps are introduced in the algorithm, as given below:

- Instead of calculating the error for each point of reference data as proposed in the fitness evaluation function, only those data values of reference data are taken which lies within a range i.e. upper and lower limit of the query data point. Suppose in the optimizing *x* and the current value of query point is 25 and if the range is ± 10, then only those values of reference data are taken for calculation of error which lies between +35 to +15. Greater the range more will be the accuracy but speed will be less, by decreasing the range the speed can be increased but this will decrease the accuracy.
- Binary search algorithm is used to find the minimum of the calculated errors. With binary search algorithm there is no need to calculate all the values of error i.e. E_1, E_2, E_3, …… E_n. Binary search algorithm searches a sorted array by repeatedly dividing the search interval in half. By using this algorithm errors in the middle value, one value above and below middle value are calculated. The algorithm narrows its search in the lower half part if error in middle value is greater than the error in value one term below the middle value while it narrows its search in the upper half part if error in middle value is greater than the error in value above the middle value. This process will continue until minimum value of error is determined. Binary search algorithm requires at most $1+\log_2 N$ iterations in comparison to N iterations in the linear search.

3.4.2.3 Termination Conditions and Reproduction

Termination conditions are required to stop the Genetic algorithm. In the present case following termination conditions have been considered and are tabulated

in Table 3.10.

Table 3.10 Termination conditions

Generations	50
Time Limit	No time limit
Fitness Limit	0
Stall Generation	15
Stall Time	15 seconds

Reproduction determines the proportion of the three types of children in the new generation. Experiments have been conducted for different values of crossover fraction and corresponding fitness values and it has been observed that any value between 0.75 to 0.8 will give the best results. So, a crossover value of 0.8 has been selected. In the present case a population of 20 individuals has to be created so the contribution of different reproduction functions is

1) Elite children = 2
2) Crossover children – 18*0.8 = 14.4 =14
3) Mutation children = 4

The flow chart of the proposed alignment using genetic algorithm and validation of image is shown in Figure 3.25. As shown in the Figure 3.25 after the initialization of different parameters like population size, crossover fraction, elite count, type of error (to find out fitness value in the present case RMSE), number of generations etc. the system optimizes the value of x, y and θ separately. Figure 3.26 shows the flow chart for the optimization of x, y and θ.

After knowing the relative linear and angular displacement between the reference image and query image from the GA based alignment algorithm, the query image has been translated and/or rotated as per the calculations and minutiae points are calculated again from the query image. Minutiae related to ridge bifurcations and ridge endings have been separated both for reference and query images. These two types of minutiae have been stored in different variables and have been arranged in the ascending order. The minutiae from the

two images are compared and a score is calculated to validate the authenticity of the person. If the score is above a particular value, then the claim of the user is authenticated, otherwise rejected.

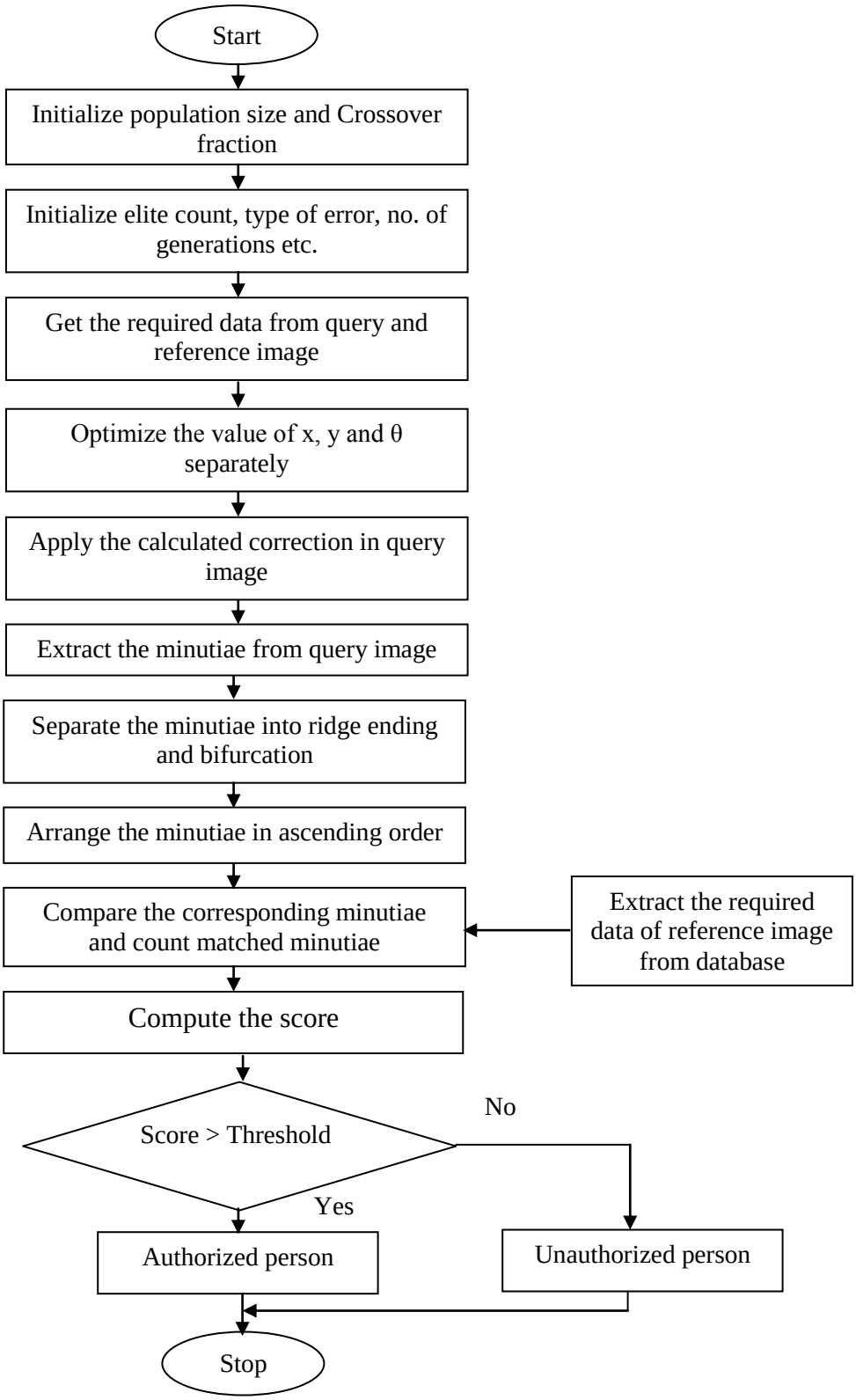


Figure 3.25 Flow chart for alignment and validation of an image

Figure 3.26 represents the flow chart to optimize x, y and θ.

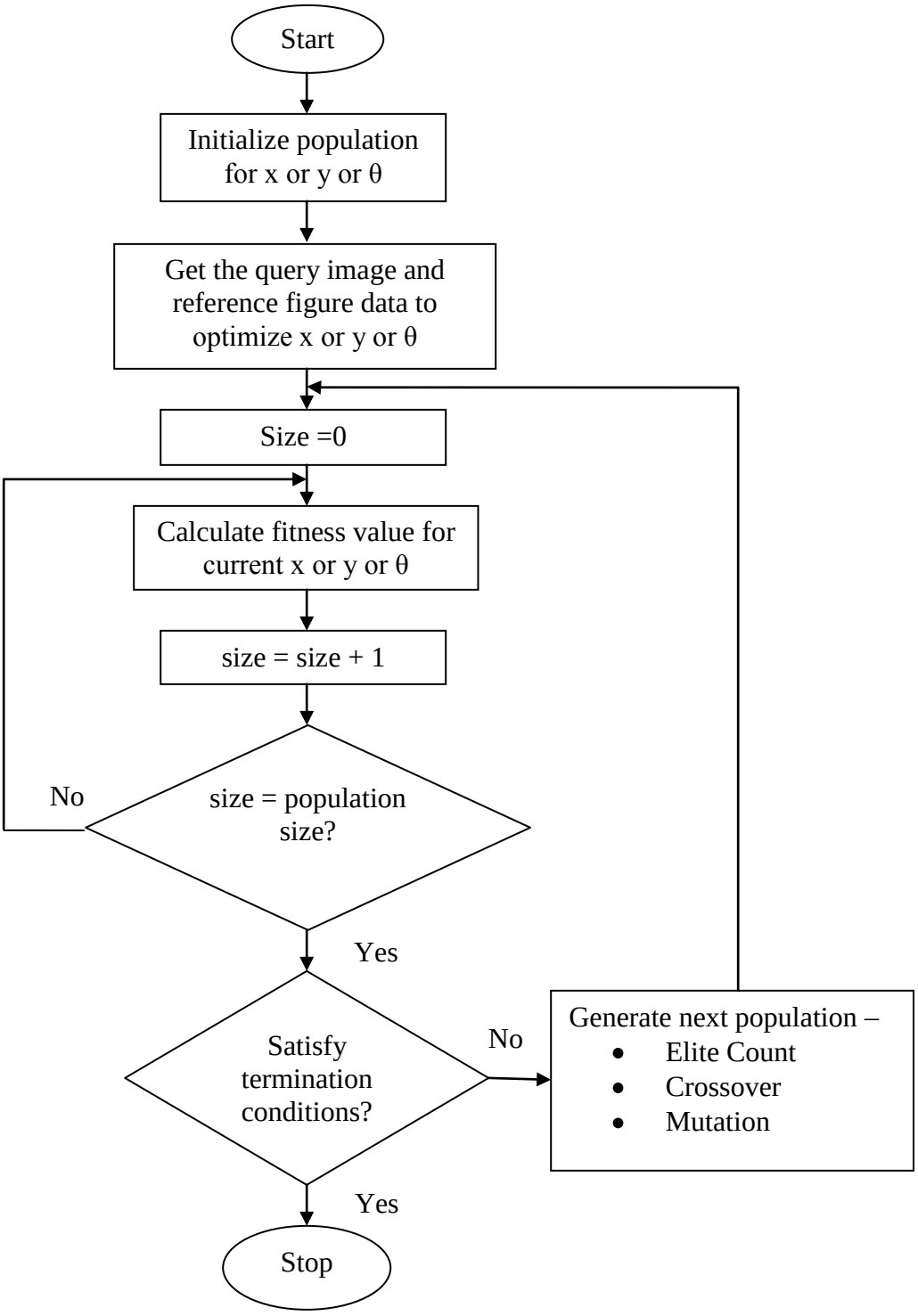


Figure 3.26 Flow chart for the optimization of x, y and θ

3.4.3 Results of Alignment and Validation

In the present work the fingerprint images from FVC2002/Db1_a database has been used to obtain the results. The fingerprint images were intentionally rotated and translated to check the performance of GA based relative alignment algorithm. Table 3.11 shows the results of the proposed alignment method for some of the fingerprint images chosen randomly from the database.

Table 3.11 Results of alignment

Fig. No.	**Simulated**			**Calculated results after GA**			**Difference**		
	x	Y	θ	x	y	θ	X	Y	θ
1_1	0	0	-2	0	0	-2	0	0	0
1_1	0	0	-3	0	0	-3	0	0	0
1_1	-1	1	2	-1	1	3	0	0	1
1_1	-5	2	3	-4	2	3	1	0	0
2_1	0	0	-5	0	0	-5	0	0	0
2_1	0	0	-14	0	0	-14	0	0	0
2_1	0	0	14	0	1	14	0	1	0
2_1	4	4	0	3	4	-1	-1	0	-1
3_1	0	0	0	-1	1	-1	-1	1	-1
3_1	4	4	0	3	3	1	-1	-1	1
3_1	11	11	0	10	10	1	-1	-1	1
3_1	0	0	-8	1	0	-7	1	0	1
4_1	0	0	5	0	0	5	0	0	0
4_1	0	0	-15	1	0	-15	1	0	0
4_1	5	5	5	5	6	4	0	1	-1
4_1	-10	-10	8	-8	-8	6	2	2	-2
5_1	-1	-1	0	0	0	1	1	1	1
5_1	9	9	0	9	9	-1	0	0	-1
5_1	15	15	2	15	13	0	0	-2	-2
5_1	0	0	-14	0	1	-14	0	1	0

6_1	0	0	1	2	0	2	2	0	1
6_1	0	0	10	1	0	12	1	0	2
6_1	-8	-8	0	-8	-8	1	0	0	1
6_1	15	15	7	12	11	7	-3	-4	0
7_1	0	0	-2	0	0	-2	0	0	0
7_1	0	0	-3	0	0	-3	0	0	0
7_1	-1	1	2	-1	2	2	0	1	0
7_1	-5	2	3	-4	3	3	1	1	0
8_1	0	0	-5	0	0	-4	0	0	1
8_1	0	0	-14	0	0	-14	0	0	0
8_1	0	0	14	2	0	14	2	0	0
8_1	4	4	0	3	4	-1	-1	0	-1
9_1	0	0	0	1	0	-1	1	0	0
9_1	4	4	0	4	3	0	0	-1	0
9_1	11	11	0	11	10	2	0	-1	2
9_1	0	0	-8	0	0	-7	0	0	1
10_1	0	0	5	0	0	5	0	0	0
10_1	0	0	-15	1	1	-15	1	1	0
10_1	5	5	5	5	6	5	0	1	0
10_1	-10	-10	10	-10	-8	9	0	2	2

Difference = Calculated results after GA - Simulated

Experiments have been performed on 3600 image database obtained by translating, rotating and translating plus rotating the fingerprints from FVC2002/Db1_a database by 1 pixel and 1 degree up to ± 15 pixel and ± 15 degree for alignment and validation using GA. The results obtained are:

i) Within ± 1 pixel and ±1 degree

When the simulated translation and rotation are within ± 5 then correct result obtained are 96% for a tolerance of ± 1 pixel translation and ±1 degree rotation. For simulated translation and rotation from ± 5 to ± 10, the results are 95% while for

simulated translation and rotation within ± 10 to ± 15, 94% results have been obtained within ± 1 pixel translation and ±1 degree rotation.

Translation and Rotation	Correct identification out of 1200 images (Within ±1 pixel and ±1 degree)	Success rate
Within ± 5	1152	96
Within ± 10	1140	95
Within ± 15	1128	94

i) Within ± 5 pixels and ± 2 degree

When the simulated translation and rotation are within ± 5 then correct result obtained are 98.5% for a tolerance of ± 1 pixel translation and ±1 degree rotation. For simulated translation and rotation from ± 5 to ± 10, the results are 98% while for simulated translation and rotation within ± 10 to ± 15, 97.5% results have been obtained within ± 5 pixel and ±2 degree.

Translation and Rotation	Correct identification out of 1200 images (Within ±5 pixel and ±2 degree)	Success rate
Within ± 5	1182	98.5
Within ± 10	1176	98
Within ± 15	1170	97.5

In about 95% of the cases the algorithm gives results in ± 1 pixel and ±1 degree. If range of tolerance is increased to ± 5 pixels and ± 2 degree accuracy becomes 98%.

3.5 Summary

Pre-processing is an essential part in minutiae based automatic fingerprint authentication systems. This step helps to extract reliable minutiae (features) from the fingerprint image. Three preprocessing steps namely segmentation, binarization and thinning

has been implemented. Segmentation has been performed by using mean and variance in a block of 16 × 16. A comparative study has been carried out to find the effect of thresholding on the fingerprint by using global thresholding and regional average thresholding. It has been concluded that the regional average thresholding is a better choice than global thresholding in case of fingerprint, which has been shown pictorially in Figure 3.10. An improved and efficient thinning algorithm has been proposed and implemented. In the proposed algorithm the 8 neighbors of a pixel in a 3 × 3 window have been arranged as 8 bits of a byte and corresponding Hexadecimal (Hex) value has been calculated. These Hex values have used to obtain a minimized Boolean expression, using standard Karnaugh Map (K map) technique. The proposed algorithm resulted in better thinned images by reducing the fingerprint image to one pixel width and makes the image rotation independent. Three different implementation steps have also been proposed and implemented to speed up the thinning process which results in the reduction of operational time by 40%. In the minutiae extraction stage a new minutiae extraction algorithm has been proposed and implemented by considering the genuine cases of minutiae only. A truth table has been formulated of the genuine minutiae cases and solved to a minimized logical expression using a well known minimization technique of Karnaugh map. The proposed method eliminates up to 25% false minutiae in the extraction stage, which remains with the crossing number method. It has also been observed that the while there is significant improvement in identification of ridge endings, only a few false ridge bifurcations case are reported. A window method of post processing has been implemented. The validity of the minutiae point has been checked by varying the size of the window. Experiments have been conducted to find out the optimum size of the window (15 in the present case) so that maximum false minutiae are eliminated and all genuine minutiae are preserved.

A new genetic algorithm based relative alignment method has been proposed and implemented to take care of the translational and rotational difference between query and reference image. All the three parameters x, y (translation) and θ (rotational) have been optimized separately and the fitness value has been calculated using the parameters from reference and query image. To speed up the process during the fitness evaluation function only those data values of reference data have been considered which lies within upper and lower limit of the query data point. The speed of the process has been further enhanced by

incorporating the binary search algorithm to find the minimum of the calculated error. The proposed method gives accurate results in 95% of the cases with a difference of ± 1 pixel and ± 1 degree while an accuracy of 98% has been obtained for the tolerance of ± 5 pixel and ± 2 degree.

CHAPTER 4

Image Based Fingerprint Verification System

Different aspects of minutiae based authentication system have been discussed in the previous chapter. The minutiae based algorithms depend upon the local discontinuities in the ridge flow pattern and requires extensive preprocessing and/or post processing operations. In this chapter an image based fingerprint verification system has been discussed. Image based matching algorithm use both the micro and macro features of a fingerprint instead of using only the minutiae locations. The present chapter includes the development of an image based verification system using the Laboratory Virtual Instrument Engineering Workbench (LabVIEW) version 6i. The effect of fingerprint image enhancement on the accuracy of the image based verification system has also been presented in this chapter.

4.1 Verification System

Verification is a process which authenticates the identity of a person by comparing the captured biometric information with his/her biometric information stored in the system. It performs one to one comparison to determine whether the identity claimed by the user is true or not. A verification algorithm consists of two steps:

1. Enrollment of the user
2. Authentication of the user

4.1.1 Enrollment of the User

In the enrollment process new users are enrolled in the system. Each user has to enter his/her name and password along with one's biometric information i.e. the fingerprint. The flow chart of enrollment type module is shown in Figure 4.1. This module has been designed in such a way that no two users should be of the same name although any user can have any password. If same name is entered that already exists in the database the algorithm will demand a new name to be entered. For the enrollment of the user a data record is to be maintained in the database containing the name, password and biometric information of the user. If simple text files are used the name and password get stored together as a single

string. Using LabVIEW data log files [170] (which are exclusively available in LabVIEW to maintain data base of records) the information regarding the user is stored in the form of clusters. Data log files makes writing and reading much faster. It also simplifies data retrieval because the original blocks of data can be read as a record without having to read all records that precede it in the file. Random access is fast and easy with Datalog files because all it needs is to access the record as the record number.

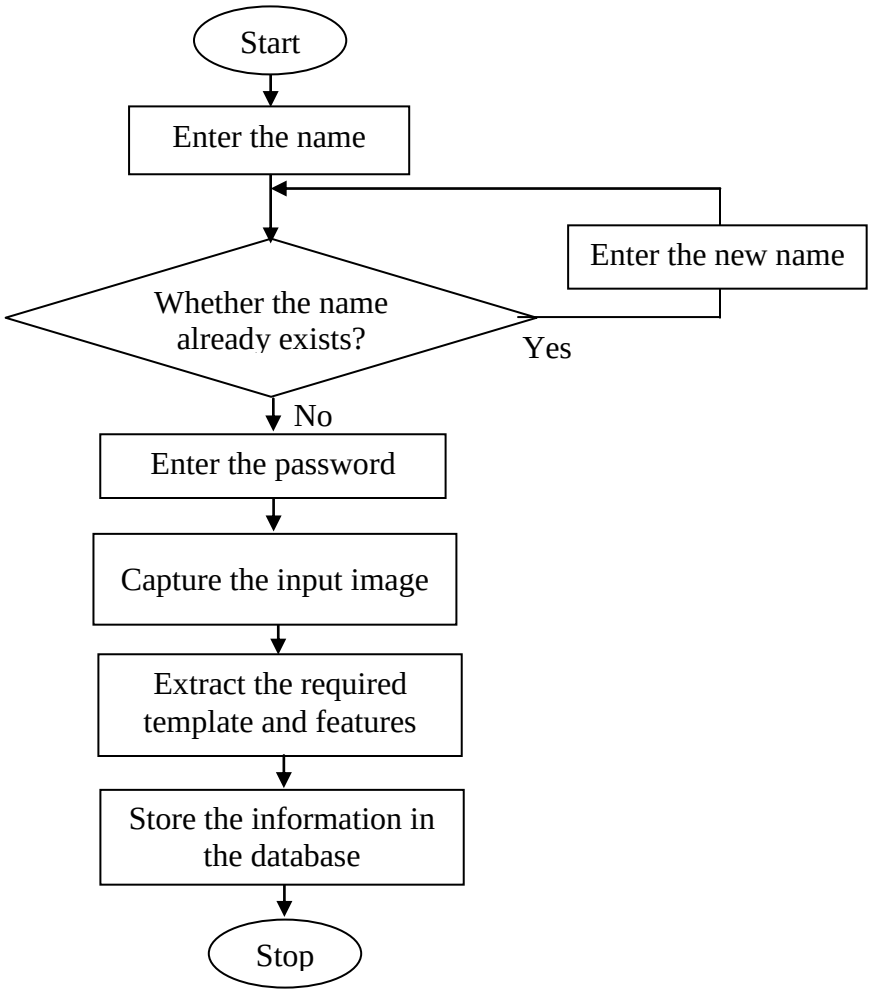


Figure 4.1 Flowchart of enrollment process

4.1.2 Authentication of the User

In the authentication step first of all the system demands the name and password of the user. The entered name and password is compared with all the enrolled users in database

to check if name and password match with any particular entry in the database. If any of the name and/or corresponding password is incorrect then the system gives a message "You are not an enrolled user" and stops. The flow chart of the authentication module is shown in the Figure 4.2.

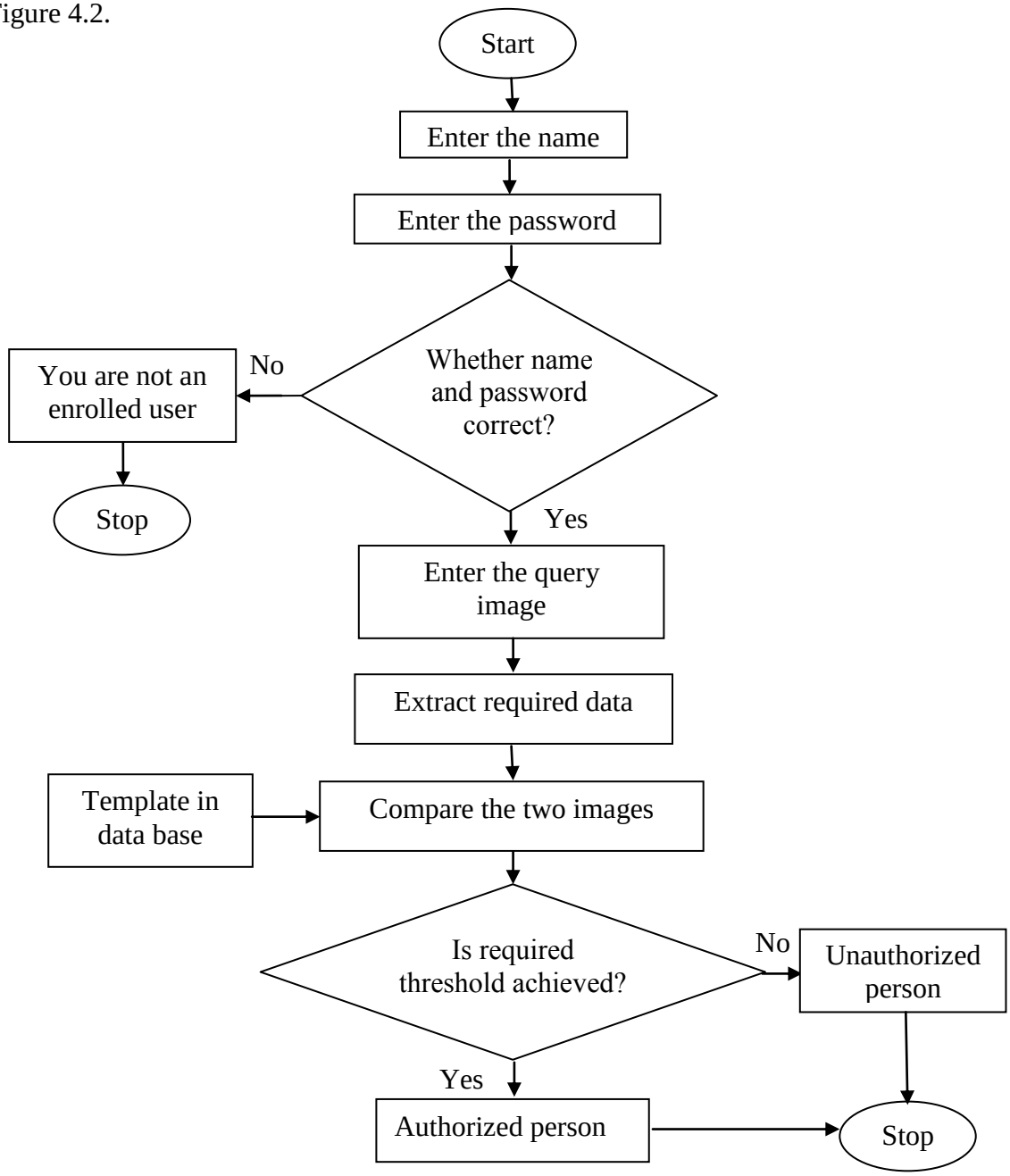


Figure 4.2 Flow chart of authentication process

As shown in the flow chart if name and password of the user are matched with any of the entry in the database then the system demands for the biometric information (fingerprint image in the present case) in question. The system extract the features from the image in

question and compares the features of the present image with the features of the user already stored in database. If matching of features from both the images lies within the accepted limit the system accepts the claim of the user, otherwise, will reject it.

The following sections explain in detail about the different blocks used and the simulation results obtained in the image based fingerprint verification system.

4.2 Template Extraction

The choice of a template is very critical for the success of the image based authentication system. A good template can be easily localized in a query image while bad template cannot be easily found in the query image. The choice of the template is influenced by its type, size and position. These factors are discussed below.

4.2.1 Type of Template

Type of the template to be extracted from the reference image is very important parameter for the success of an image based authentication system. Following points must be kept in mind for the while selecting the type of the template in an image based authentication system [171].

- The template should be asymmetric enough so that it can be uniquely identified at a certain orientation.
- Complex templates will take longer to match than very simple ones. However, too simple template may result in spurious matches and increased false acceptance rate.
- The template should contain enough detail to fix its spatial position in the image. To do this, it needs to contain both vertical and horizontal features.

4.2.2 Size of Template

In order to overcome the problem of high computational complexity of the correlation based methods a small size template should be extracted from the reference image and to be correlated with each and every point in the query image. Size of the extracted template is very critical because size of the template affects the speed and accuracy of the system. Too small size template may not provide enough distinction [61]; on the other hand if entire fingerprint is taken as a template then apart from the speed limitation, the elastic deformation of the query image may cause serious errors.

4.2.3 Position of Template

Position of the template i.e. the point from where the template is to be extracted is also very crucial. The core or delta points in a fingerprint image may act as reference point. However, when these points can not be reliably detected or they are very near to the border of the fingerprint area, the extracted features of the input fingerprint may be incomplete or incompatible with respect to the template.

In the literature minutiae based, coherence based and correlation based three different template selection methods have been discussed. In minutiae based approach, templates around the minutiae point are extracted to locate the template in the query image correctly and efficiently [172]. This method suffers with all the problems of minutiae based systems, moreover, time will be required to extract the minutiae points. In the coherence (a measure of direction for local gradients) based template selection method those templates are chosen which have low coherence values [61]. The advantage of this system is that it also includes the minutiae points because the area around the minutiae points contains more gray scale gradient orientations which results in a lower coherence. But the disadvantage of this method is that the noisy areas also represent the low coherence so it becomes difficult to differentiate between the area of interest and the noisy area. In correlation based template selection method templates are selected depending upon their dissimilarity at other positions in the same fingerprint. If the dissimilarity of the template at its original position and at all the other positions in an image is more then it will be a good template because this particular template contains enough distinction to give the accurate results. If the dissimilarity is less then it is not a useful template. This method of template selection suffers from the limitation of computational requirements.

In the present work, a square template of size 50×50, 100×100 and 200×200 pixels has been considered for extraction. The reference templates are extracted starting from the center of the image and the selection of the template depends upon its value of the standard deviation. The standard deviation of template k of size $W \times W$ is given by:

$$\sigma(k) = \left[\frac{1}{W^2} \sum_{i=0}^{W-1} \sum_{j=0}^{W-1} \left(I(i,j) - M(k) \right)^2 \right]^{1/2} \qquad (4.1)$$

Where, $M(k)$ = Mean of block k and $I(i,j)$ = Value at pixel (i,j)

Since standard deviation is a very good measure of dispersion of the data [173]. More the value of standard deviation more is the distinction between the components of the template and more time it will take to learn while if the value of the standard deviation is less then the distinction in the components of the template is less which may affect the accuracy of the system. So, a compromise has to be made between the accuracy and speed of the system for the choice of the standard deviation of the template. Experimentally it has been observed that the standard deviation of 300 units , 450 units and 600 units gives good results for the template image size of 50×50, 100×100 and 200×200 pixels respectively. The flow chart of template extraction process has been shown in Figure 4.3.

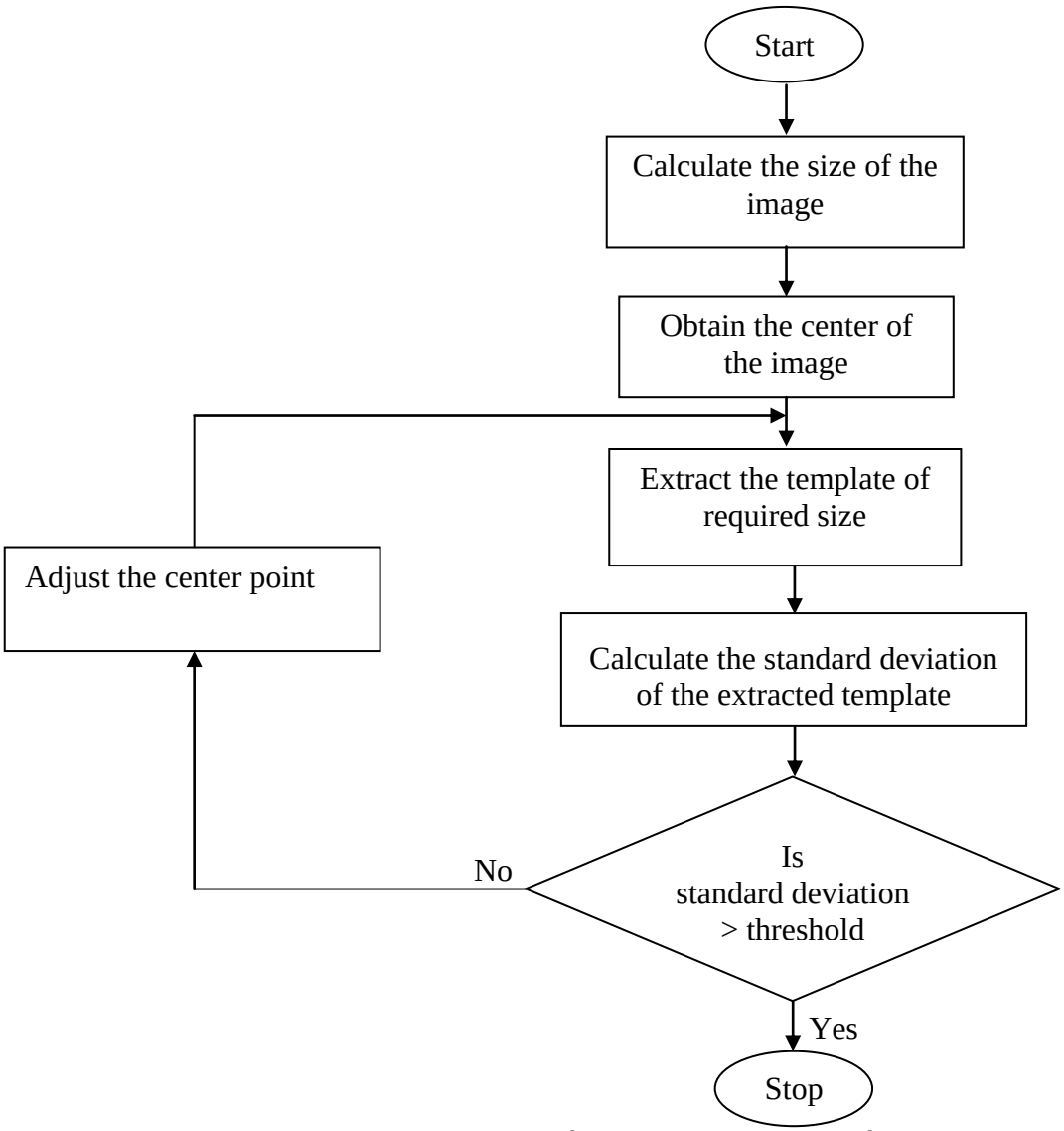


Figure 4.3 Flow chart for template extraction from the image

As shown in the flow chart if, the extracted image does not provide the required standard deviation then a new window has to be extracted. This has been done by moving the center of the extraction window to $1/4^{th}$ of the template size in x and y direction simultaneously. The standard deviation of the new window has to be calculated again. This process continuous until the template of required standard deviation has been obtained.

4.3 Feature Extraction and Learning

The feature extraction and learning phase of image based verification system involves analyzing the template image to find features that can be exploited for efficient matching performance. The traditional grayscale correlation methods have no learning phase. In traditional methods the template is simply compared to every possible location in the image via a 2D correlation. The main drawback of this type of method is the huge computational effort required [174]. With a learning phase the number of calculations can be reduced by sub-sampling of the template image. This stage should extract the information about the overall structure of the image, identifies & extracts features of the template that are rotation independent & scale independent. The extracted features will be useful for localizing the match. The information extracted by this stage will be used for comparison with the data of the query image, during the matching stage. The feature extraction stage is divided into following two parts

(i) Translation and rotation

(ii) Sampling and edge detection

4.3.1 Translation and Rotation

Translation and rotation between the reference and query fingerprints is a major issue which must be taken into account for the success of an image based fingerprint authentication system. In order to take care of the rotation and translation the circular intensity profile of the template image has been calculated. Figure 4.4 (a) depicts the original image 1_1 of database FVC 2002/ Db_1a while Figure 4.4 (b) depicts the image 1_1 with 14 pixels translation in x and y direction. Figure 4.5 shows the circular intensity profile of the selected region indicated by the red circle in the original image. Figure 4.6 shows the circular intensity profile of the selected region indicated by the red circle in the translated image.

(a) (b)

Figure 4.4 (a) Original image 1_1 (b) Image 1_1 with 14 pixels translation in x and y direction

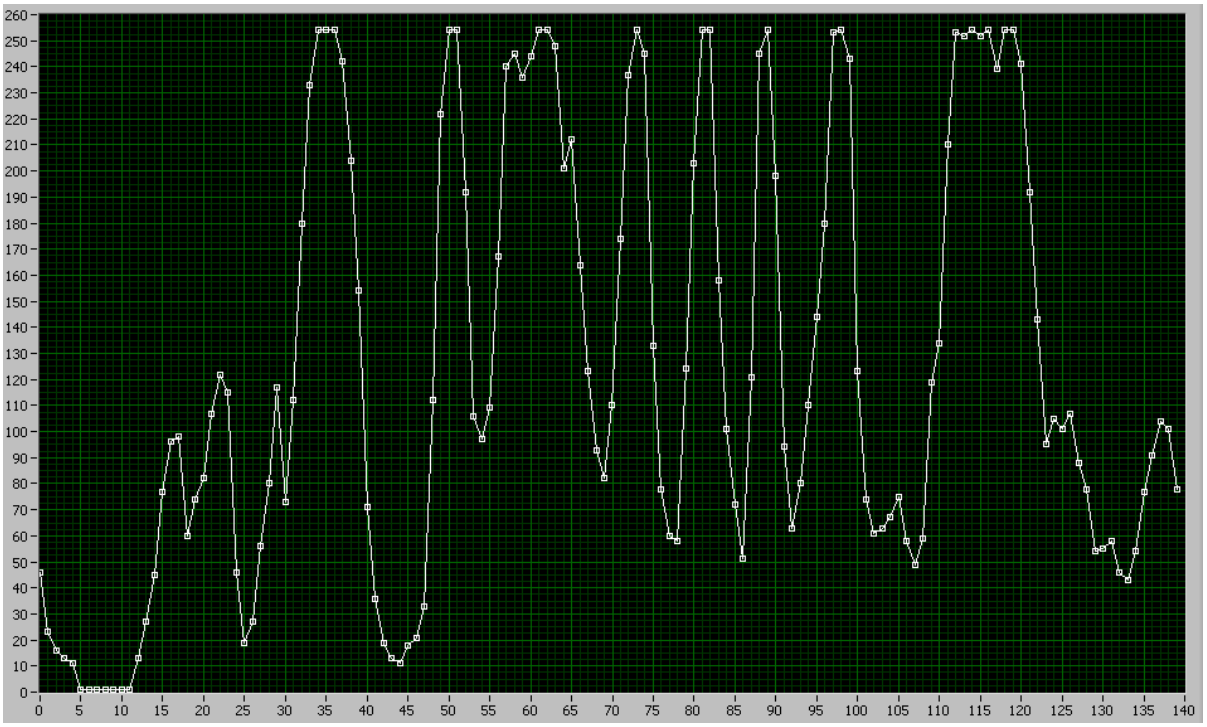


Figure 4.5 Circular intensity profile of original image 1_1

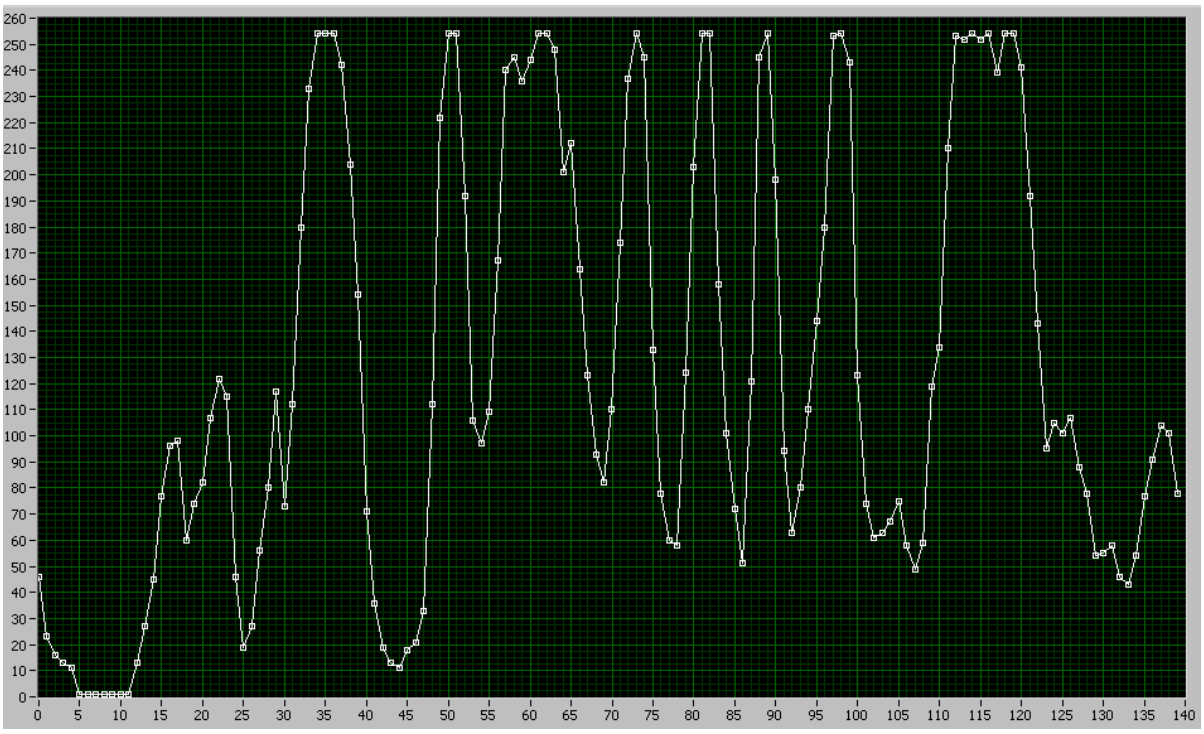


Figure 4.6 Circular intensity profile of image 1_1 with translation of 14 pixels in x and y direction

The comparison of Figure 4.5 and 4.6 reveals that the circular intensity profile of both original and translated image is same. The circular intensity profile of rotated image will also be same as that of the original image, but it will be shifted to right or left depending upon the amount and direction of rotation.

4.3.2 Sampling and Edge Detection

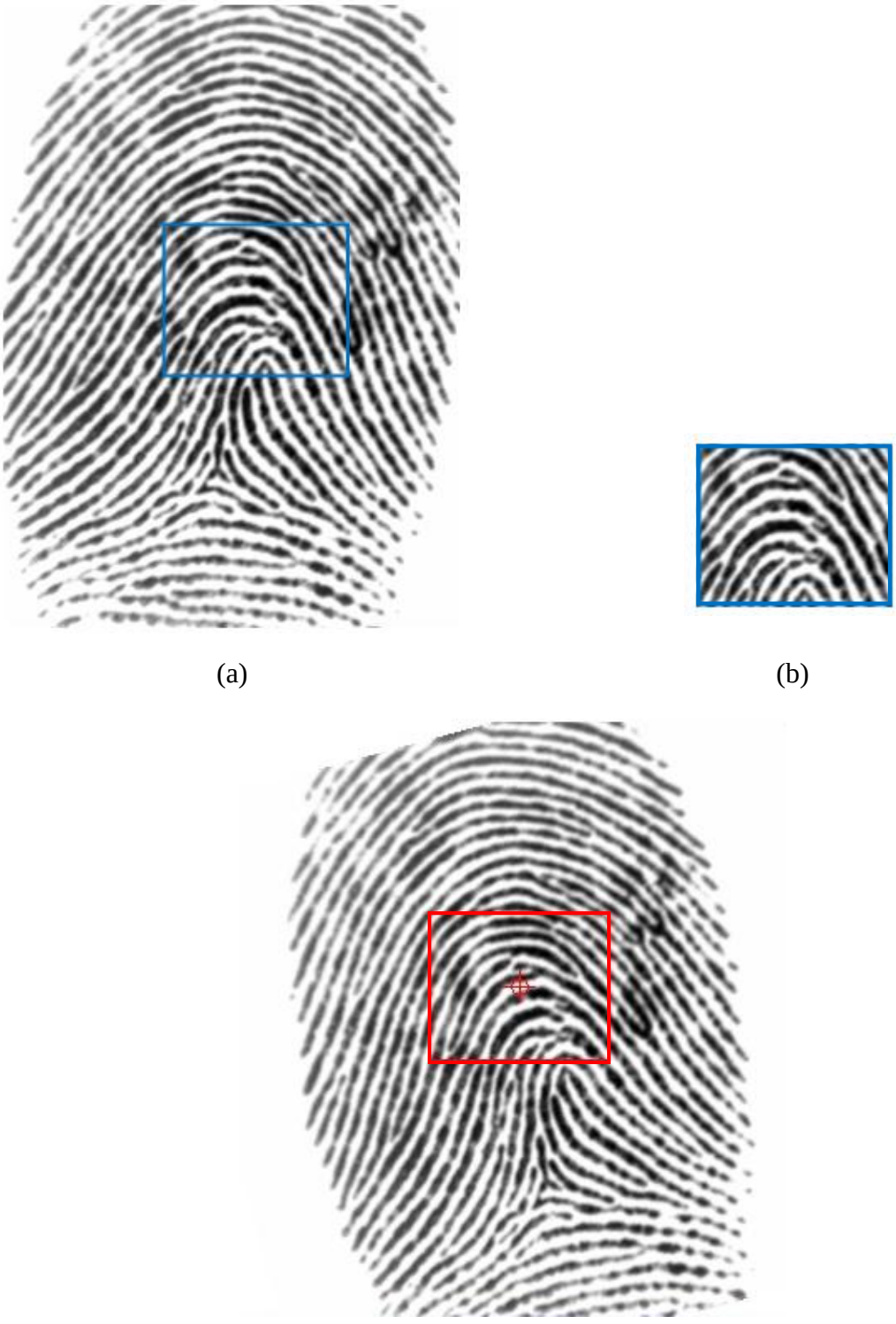
In order to take care the problem of high computational complexity present in the traditional correlation based methods an image understanding technique has been used. Image understanding refers to the image processing technique that extracts the overall structure of the template image. This has been done by using the quasi-random sub sampling operation in which pixels are analyzed by checking their surrounding neighborhood for uniformity and each pixel is classified according to how large its surrounding neighborhood is uniform (i.e. 3×3, 5×5 and so on)[175]. Quasi- random sub sampling reduces the amount of information needed to fully characterize an image or pattern, which speeds up the

searching process. Also, extracting useful information from a template and removing the redundant and noisy information provides a more reliable and accurate result.

At last, Sobel edge detector has been applied on the template image to find out the strong edge points i.e. the edge points having the magnitude greater than a threshold value. These details will be helpful for the fine tuning the location of the matched template in the query image. This learning phase is quite complex and calculations may take several seconds to perform. But, this phase needs to be done once per template [175].

4.4 Matching

During the matching stage the required pattern is searched in the query image by using the information from the learning phase. The matching phase consists in sliding the sampling structure over the query image and look for the rotated or translated version of the circular intensity profile of the reference (template) image stored in the file. Several candidate matches are possible during this stage. In order to speed up the process the search space may be restricted by specifying the degree of rotation. The system then considers each candidate separately to find out the overall structure of the template. This has been done by using the quasi-random pixels extracted during the feature extraction stage and performing the cross correlation with all the possible candidates identified by the circular intensity profile. A score is calculated for each candidate and candidates for higher score are considered for matching with the edge detection results of the learning phase to fine tune the location of each match. A score is again determined using cross correlation to determine the degree of match between the two images and to validate the claim of the user. Figure 4.7 (a) shows the fingerprint image 1_1 of database FVC 2002/Db1_a. The square box with the blue colour indicate the portion of the image to be extracted for learning as shown in Figure 4.7 (b). Image in Figure 4.7 (c) is the query image, which is the translated and rotated by 15 pixels (x and y direction both) and 15 degree respectively. The red box in Figure 4.7 (c) indicates the matched region with the template in the query image.



(a) (b)

(c)

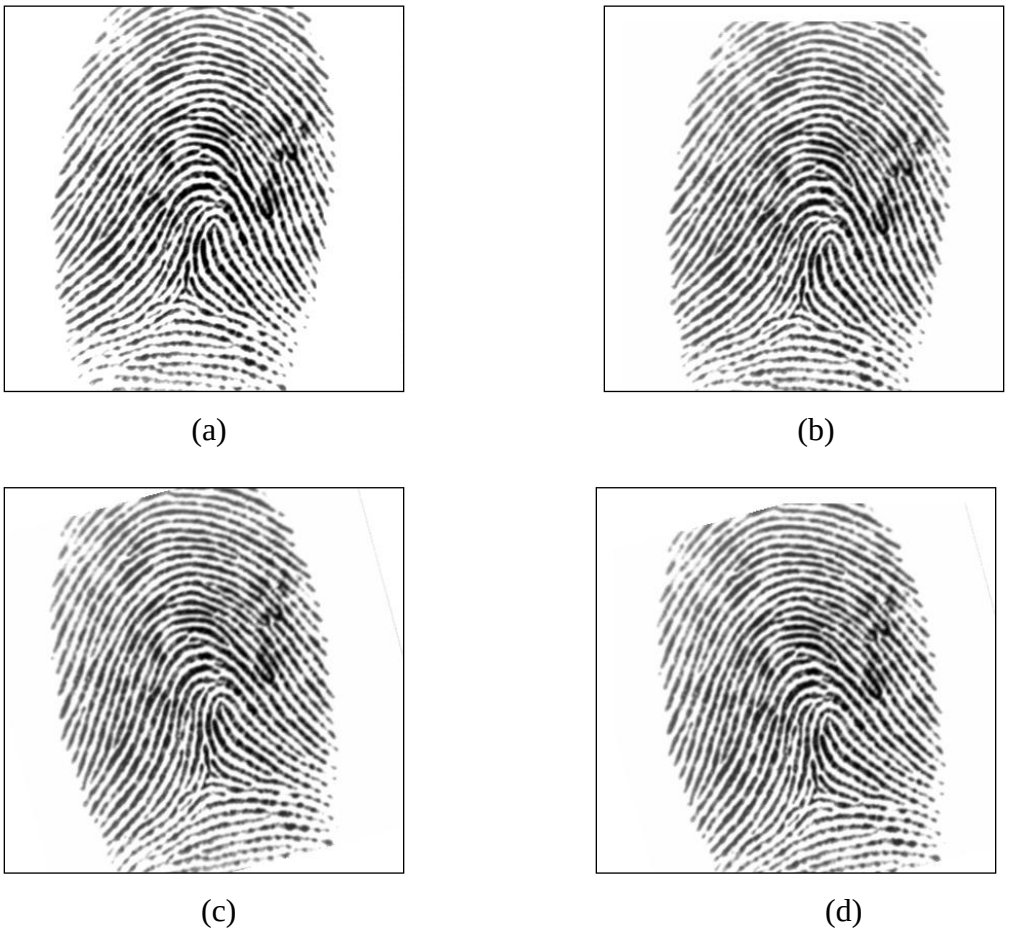
Figure 4.7 (a) Fingerprint image 1_1 of database FVC 2002/Db1_a (b) Extracted portion of the image (c) Query image (red box indicates the matched portion in query image)

4.5 Database

In the present work the fingerprint images from FVC2002/Db1_a has been used to obtain the results. Further, a data base has been created by:

- Translating the fingerprint images by 1 pixel in both X and Y direction
- Rotating the fingerprint images by 1 degree
- Both translating and rotating the images by 1 pixel and 1 degree

The images are translated and rotated up to ± 15 pixels and ± 15 degree. Figure 4.8 shows the original image 1_1 of FVC2002/Db1_a, its translated, rotated and translated plus rotated versions.



(a) (b)

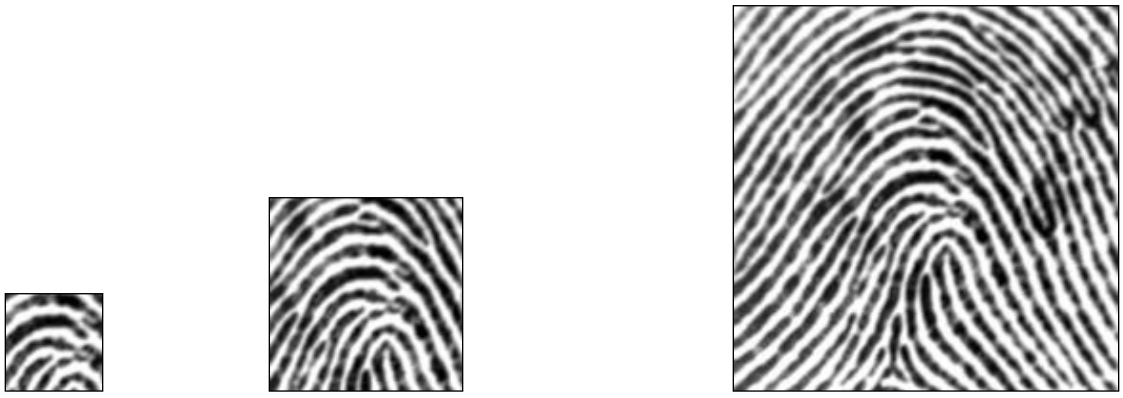
(c) (d)

Figure 4.8 (a) Original Image (b) Translated Image in X and Y direction (c) Rotated Image (d) Rotated plus translated image

In this way for every selected image of FVC2002/Db1_a 90 (30 translated, 30 rotated and 30 translated plus rotated) images have been obtained.

4.6 Results

Two performance measures namely, false rejection rate and false acceptance rate have been calculated for different images, with different thresholds and template sizes. Experiments have been performed by considering template size of 50×50, 100×100 and 200×200 pixels respectively extracted from the image as explained in section 4.3. Figure 4.9 shows the extracted images of template size 50×50, 100×100 and 200×200 pixels respectively from the image 1_1 of FVC2002/Db1_a database.



(a) (b) (c)

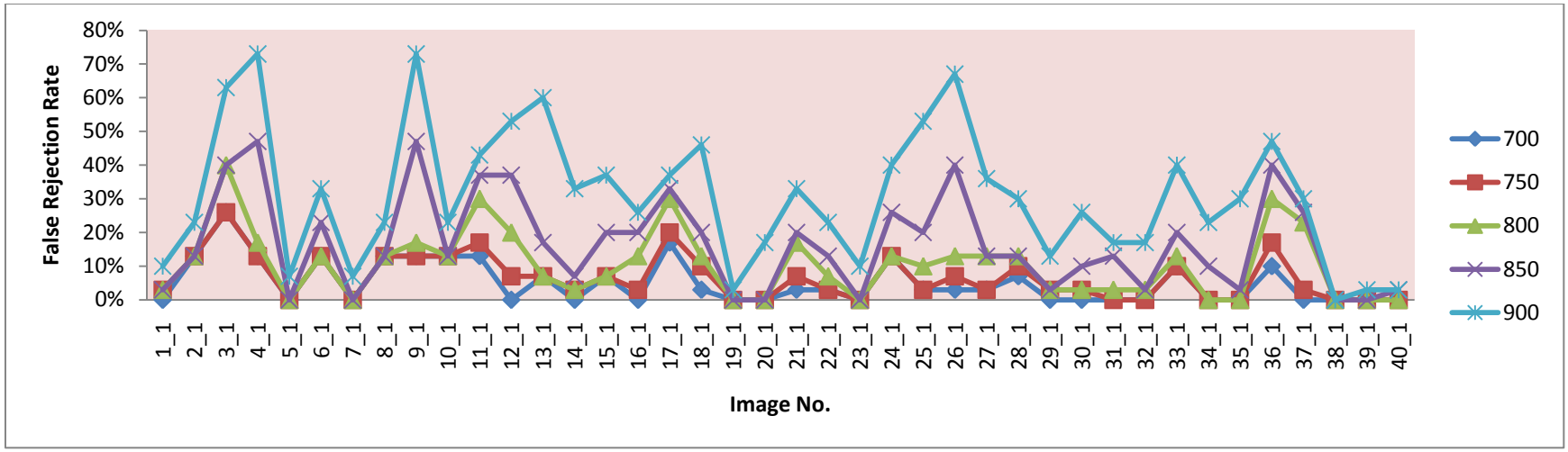
Figure 4.9 Template size of (a) 50×50 pixels (b) 100×100 pixels (c) 200×200 pixels extracted from image 1_1 of FVC2002/Db1_a database

4.6.1 False Rejection Rate

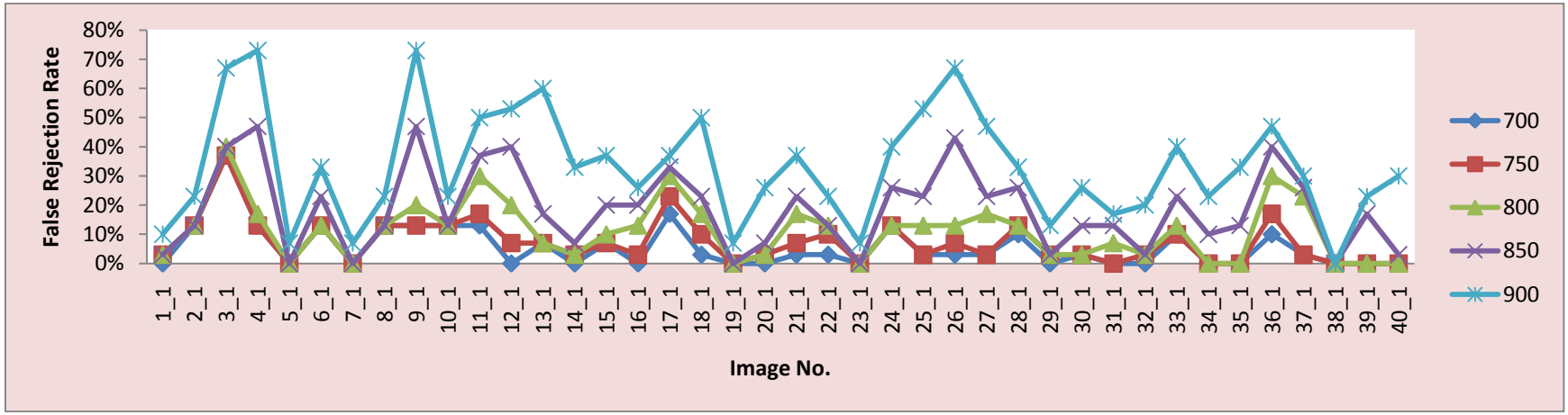
False rejection rate also known as false non-match rate (FNMR) is the error which occurs when the system considers two biometric measurements from the same source (fingerprint in the present case) to be from the different sources (fingerprints). Each fingerprint image of different person in the database is compared with all 90 (30 translated, 30 rotated and 30 translated plus rotated) images of the same person to find out the false non-match rate (FNMR). The simulation results obtained for learning image sizes of 200×200, 100×100 and 50×50 have been tabulated in Table 4.1, Table 4.2 and Table 4.3 respectively. Figure 4.10, Figure 4.11 and Figure 4.12 shows the graphical representation of the obtained results. Table 4.4, Table 4.5 and Table 4.6 shows the consolidated results of all the fingers in the database for learning image sizes of 200×200, 100×100 and 50×50 respectively.

Table 4.1 False rejection rate for learning image size 200× 200

Sr. No.	Image No.	Translated					Rotated					Translated plus rotated				
		Threshold					Threshold					Threshold				
		700	750	800	850	900	700	750	800	850	900	700	750	800	850	900
1	**1_1**	0%	0%	0%	0%	0%	0%	3%	3%	3%	10%	0%	3%	3%	3%	10%
2	**2_1**	0%	0%	0%	0%	0%	13%	13%	13%	13%	23%	13%	13%	13%	13%	23%
3	**3_1**	0%	0%	0%	0%	0%	27%	27%	40%	40%	63%	37%	37%	40%	40%	67%
4	**4_1**	0%	0%	0%	0%	0%	13%	13%	17%	47%	73%	13%	13%	17%	47%	73%
5	**5_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%	0%	0%	0%	0%	7%
6	**6_1**	0%	0%	0%	0%	0%	13%	13%	13%	23%	33%	13%	13%	13%	23%	33%
7	**7_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%	0%	0%	0%	0%	7%
8	**8_1**	0%	0%	0%	0%	0%	13%	13%	13%	13%	23%	13%	13%	13%	13%	23%
9	**9_1**	0%	0%	0%	0%	0%	13%	13%	17%	47%	73%	13%	13%	20%	47%	73%
10	**10_1**	0%	0%	0%	0%	0%	13%	13%	13%	13%	23%	13%	13%	13%	13%	23%
11	**11_1**	0%	0%	0%	0%	0%	13%	17%	30%	37%	43%	13%	17%	30%	37%	50%
12	**12_1**	0%	0%	0%	0%	0%	0%	7%	20%	37%	53%	0%	7%	20%	40%	53%
13	**13_1**	0%	0%	0%	0%	0%	7%	7%	7%	17%	60%	7%	7%	7%	17%	60%
14	**14_1**	0%	0%	0%	0%	0%	0%	3%	3%	7%	33%	0%	3%	3%	7%	33%
15	**15_1**	0%	0%	0%	0%	0%	7%	7%	7%	20%	37%	7%	7%	10%	20%	37%
16	**16_1**	0%	0%	0%	0%	0%	0%	3%	13%	20%	27%	0%	3%	13%	20%	27%
17	**17_1**	0%	0%	0%	0%	0%	17%	20%	30%	33%	37%	17%	23%	30%	33%	37%
18	**18_1**	0%	0%	0%	0%	0%	3%	10%	13%	20%	46%	3%	10%	17%	23%	50%
19	**19_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	7%
20	**20_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	17%	0%	3%	3%	7%	27%
21	**21_1**	0%	0%	0%	0%	0%	3%	7%	17%	20%	33%	3%	7%	17%	23%	37%
22	**22_1**	0%	0%	0%	0%	0%	3%	3%	7%	13%	23%	3%	10%	13%	13%	23%
23	**23_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	10%	0%	0%	0%	0%	7%
24	**24_1**	0%	0%	0%	0%	0%	13%	13%	13%	27%	40%	13%	13%	13%	27%	40%
25	**25_1**	0%	0%	0%	0%	0%	3%	3%	10%	20%	53%	3%	3%	13%	23%	53%
26	**26_1**	0%	0%	0%	0%	0%	3%	7%	13%	40%	67%	3%	7%	13%	43%	67%
27	**27_1**	0%	0%	0%	0%	0%	3%	3%	13%	13%	37%	3%	3%	17%	23%	47%
28	**28_1**	0%	0%	0%	0%	0%	7%	10%	13%	13%	30%	10%	13%	13%	27%	33%
29	**29_1**	0%	0%	0%	0%	0%	0%	3%	3%	3%	13%	0%	3%	3%	3%	13%
30	**30_1**	0%	0%	0%	0%	0%	0%	3%	3%	10%	27%	3%	3%	3%	13%	27%
31	**31_1**	0%	0%	0%	0%	0%	0%	0%	3%	13%	17%	0%	0%	7%	13%	17%
32	**32_1**	0%	0%	0%	0%	0%	0%	0%	3%	3%	17%	0%	3%	3%	3%	20%
33	**33_1**	0%	0%	0%	0%	0%	10%	10%	13%	20%	40%	10%	10%	13%	23%	40%
34	**34_1**	0%	0%	0%	0%	0%	0%	0%	0%	10%	23%	0%	0%	0%	10%	23%
35	**35_1**	0%	0%	0%	0%	0%	0%	0%	0%	3%	30%	0%	0%	0%	13%	33%
36	**36_1**	0%	0%	0%	0%	0%	10%	17%	30%	40%	47%	10%	17%	30%	40%	47%
37	**37_1**	0%	0%	0%	0%	0%	0%	3%	23%	27%	30%	3%	3%	23%	27%	30%
38	**38_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
39	**39_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	17%	23%
40	**40_1**	0%	0%	0%	0%	0%	0%	0%	0%	3%	3%	0%	0%	0%	3%	30%



(a)



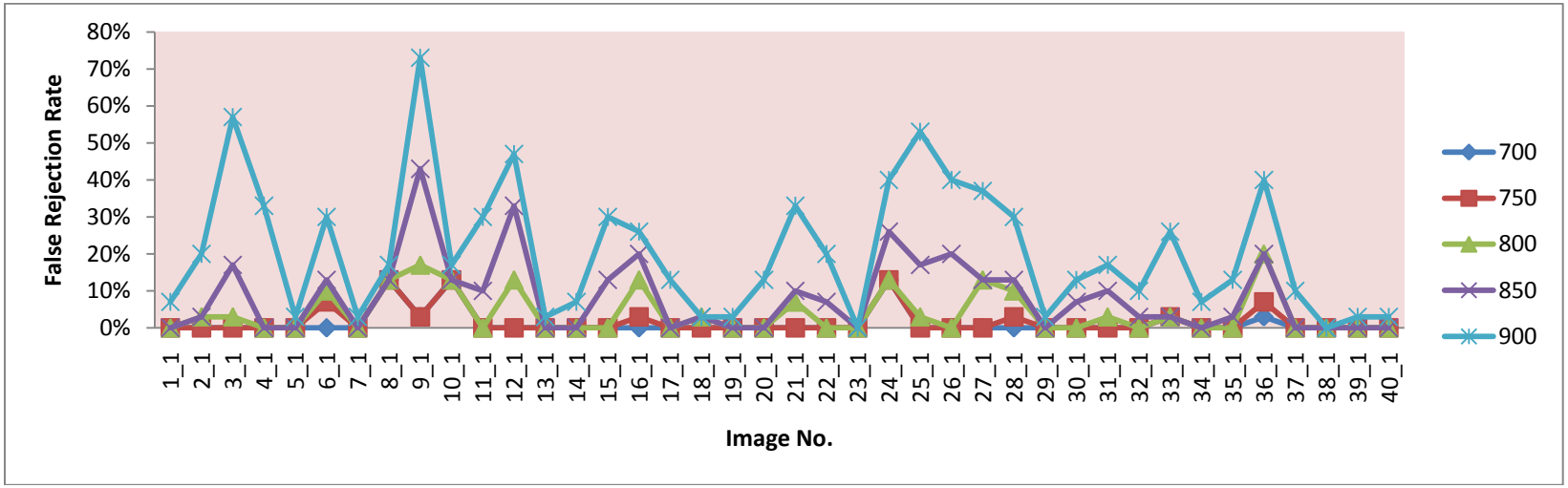
(b)

Figure 4.10 False rejection rate of different images for various thresholds with learning image size 200× 200

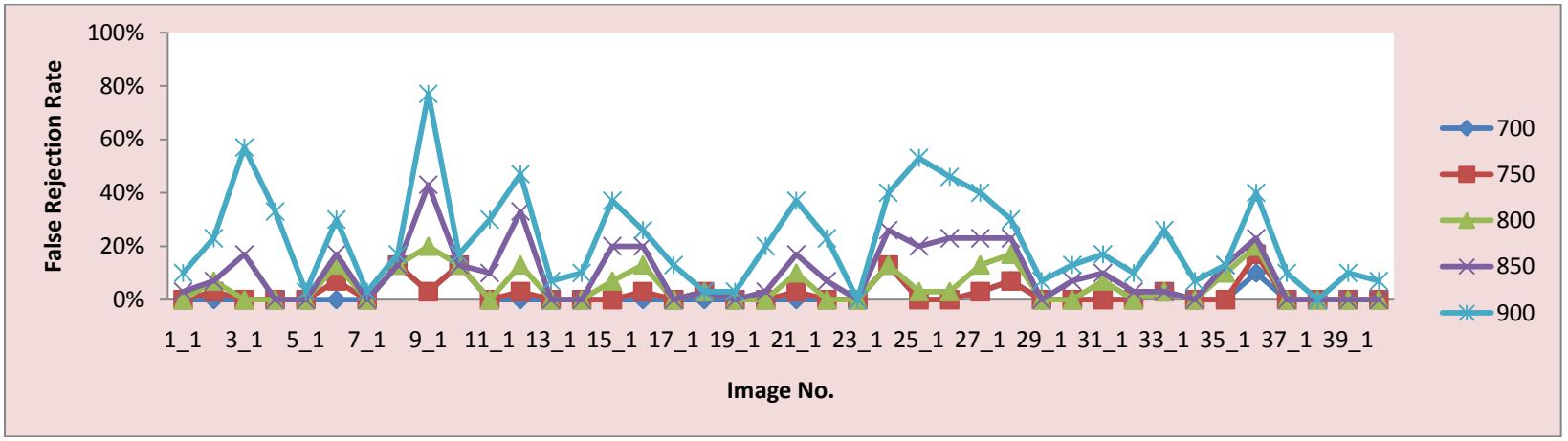
(a) Rotation only (b) Rotation and translation

Table 4.2 False rejection rate for learning image size 100× 100

Sr. No.	Image No.	Translated					Rotated					Translated plus rotated				
		Threshold					Threshold					Threshold				
		700	750	800	850	900	700	750	800	850	900	700	750	800	850	900
1	**1_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%	0%	0%	0%	3%	10%
2	**2_1**	0%	0%	0%	0%	0%	0%	0%	3%	3%	20%	0%	3%	7%	7%	23%
3	**3_1**	0%	0%	0%	0%	0%	0%	0%	3%	17%	57%	0%	0%	0%	17%	57%
4	**4_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	33%	0%	0%	0%	0%	33%
5	**5_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	3%
6	**6_1**	0%	0%	0%	0%	0%	0%	7%	10%	13%	30%	0%	7%	13%	17%	30%
7	**7_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	3%
8	**8_1**	0%	0%	0%	0%	0%	13%	13%	13%	13%	17%	13%	13%	13%	13%	17%
9	**9_1**	0%	0%	0%	0%	0%	3%	3%	17%	43%	73%	3%	3%	20%	43%	77%
10	**10_1**	0%	0%	0%	0%	0%	13%	13%	13%	13%	17%	13%	13%	13%	13%	17%
11	**11_1**	0%	0%	0%	0%	0%	0%	0%	0%	10%	30%	0%	0%	0%	10%	30%
12	**12_1**	0%	0%	0%	0%	0%	0%	0%	13%	33%	47%	0%	3%	13%	33%	47%
13	**13_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	7%
14	**14_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%	0%	0%	0%	0%	10%
15	**15_1**	0%	0%	0%	0%	0%	0%	0%	0%	13%	30%	0%	0%	7%	20%	37%
16	**16_1**	0%	0%	0%	0%	0%	0%	3%	13%	20%	27%	0%	3%	13%	20%	27%
17	**17_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	13%	0%	0%	0%	0%	13%
18	**18_1**	0%	0%	0%	0%	0%	0%	0%	3%	3%	3%	0%	3%	3%	3%	3%
19	**19_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	3%
20	**20_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	13%	0%	0%	0%	3%	20%
21	**21_1**	0%	0%	0%	0%	0%	0%	0%	7%	10%	33%	0%	3%	10%	17%	37%
22	**22_1**	0%	0%	0%	0%	0%	0%	0%	0%	7%	20%	0%	0%	0%	7%	23%
23	**23_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
24	**24_1**	0%	0%	0%	0%	0%	13%	13%	13%	27%	40%	13%	13%	13%	27%	40%
25	**25_1**	0%	0%	0%	0%	0%	0%	0%	3%	17%	53%	0%	0%	3%	20%	53%
26	**26_1**	0%	0%	0%	0%	0%	0%	0%	0%	20%	40%	0%	0%	3%	23%	46%
27	**27_1**	0%	0%	0%	0%	0%	0%	0%	13%	13%	37%	3%	3%	13%	23%	40%
28	**28_1**	0%	0%	0%	0%	0%	0%	3%	10%	13%	30%	7%	7%	17%	23%	30%
29	**29_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	7%
30	**30_1**	0%	0%	0%	0%	0%	0%	0%	0%	7%	13%	0%	0%	0%	7%	13%
31	**31_1**	0%	0%	0%	0%	0%	0%	0%	3%	10%	17%	0%	0%	7%	10%	17%
32	**32_1**	0%	0%	0%	0%	0%	0%	0%	0%	3%	10%	0%	0%	0%	3%	10%
33	**33_1**	0%	0%	0%	0%	0%	3%	3%	3%	3%	26%	3%	3%	3%	3%	26%
34	**34_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%	0%	0%	0%	0%	7%
35	**35_1**	0%	0%	0%	0%	0%	0%	0%	0%	3%	13%	0%	0%	10%	13%	13%
36	**36_1**	0%	0%	0%	0%	0%	3%	7%	20%	20%	40%	10%	17%	20%	23%	40%
37	**37_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	10%	0%	0%	0%	0%	10%
38	**38_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
39	**39_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	10%
40	**40_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	7%



(a)



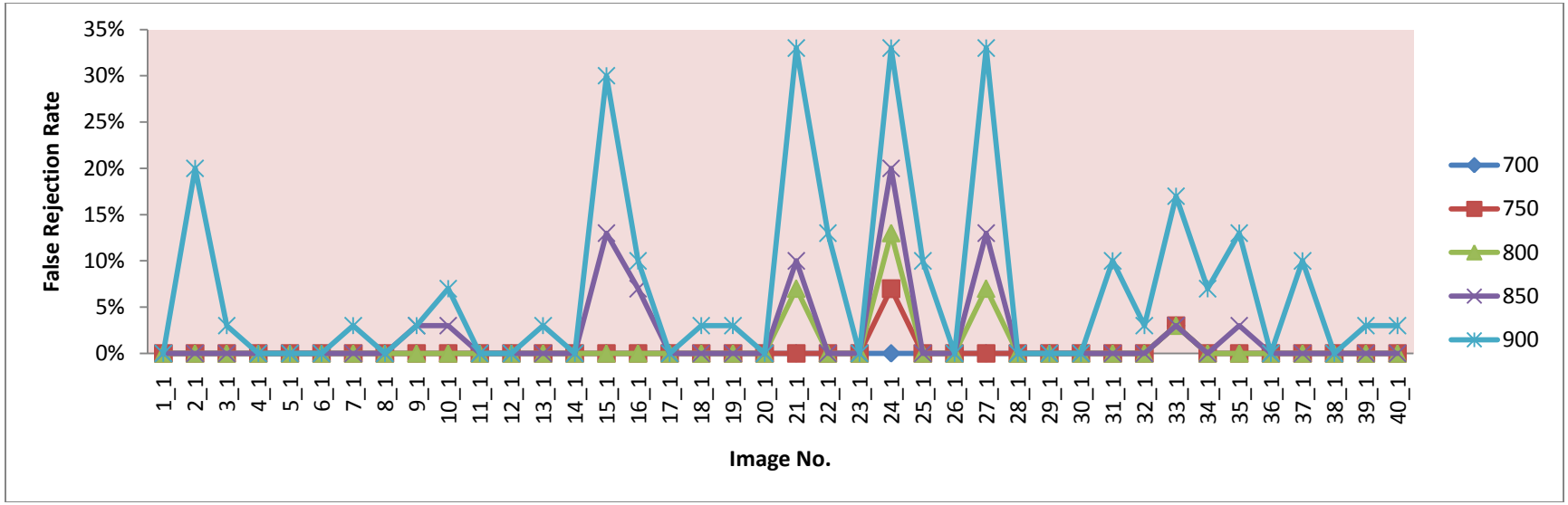
(b)

Figure 4.11 False rejection rate of different images for various thresholds with learning image size 100× 100

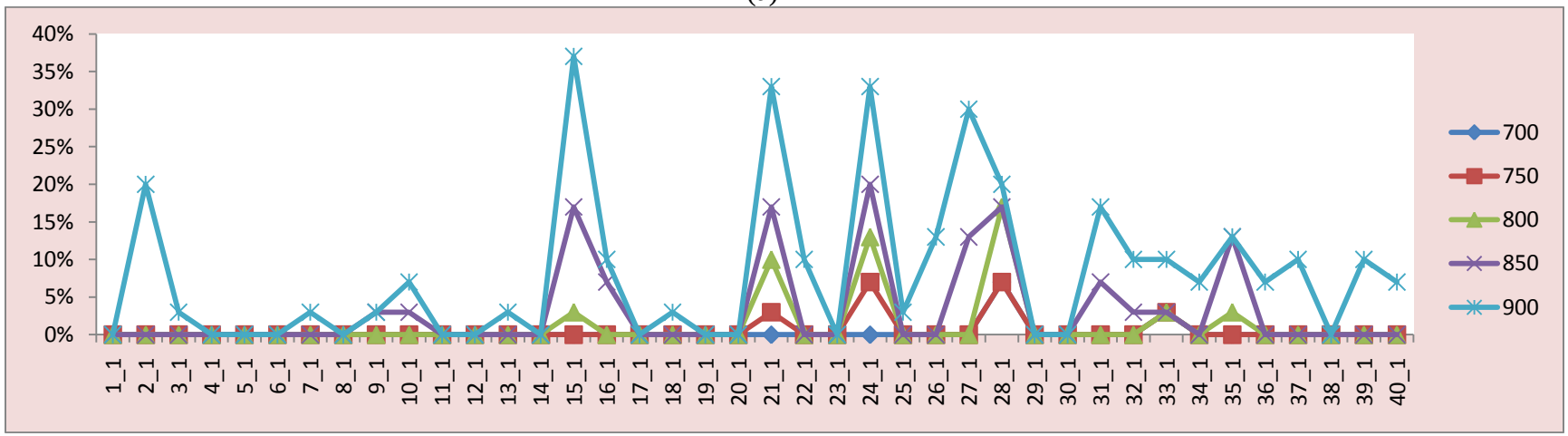
(a) Rotation only (b) Rotation and translation

Table 4.3 False rejection rate for learning image size 50× 50

Sr. No.	Image No.	Translated					Rotated					Translated plus rotated				
		Threshold					Threshold					Threshold				
		700	750	800	850	900	700	750	800	850	900	700	750	800	850	900
1	**1_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
2	**2_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	20%	0%	0%	0%	0%	20%
3	**3_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	3%
4	**4_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
5	**5_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
6	**6_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
7	**7_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	3%
8	**8_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
9	**9_1**	0%	0%	0%	0%	0%	0%	0%	0%	3%	3%	0%	0%	0%	3%	3%
10	**10_1**	0%	0%	0%	0%	0%	0%	0%	0%	3%	7%	0%	0%	0%	3%	7%
11	**11_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
12	**12_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
13	**13_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	3%
14	**14_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
15	**15_1**	0%	0%	0%	0%	0%	0%	0%	0%	13%	30%	0%	0%	3%	17%	37%
16	**16_1**	0%	0%	0%	0%	0%	0%	0%	0%	7%	10%	0%	0%	0%	7%	10%
17	**17_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
18	**18_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	3%
19	**19_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	0%
20	**20_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
21	**21_1**	0%	0%	0%	0%	0%	0%	0%	7%	10%	33%	0%	3%	10%	17%	33%
22	**22_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	13%	0%	0%	0%	0%	10%
23	**23_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
24	**24_1**	0%	0%	0%	0%	0%	0%	7%	13%	20%	33%	0%	7%	13%	20%	33%
25	**25_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	10%	0%	0%	0%	0%	3%
26	**26_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	13%
27	**27_1**	0%	0%	0%	0%	0%	0%	0%	7%	13%	33%	0%	0%	0%	13%	30%
28	**28_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%	7%	17%	17%	20%
29	**29_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
30	**30_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
31	**31_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	10%	0%	0%	0%	7%	17%
32	**32_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	3%	10%
33	**33_1**	0%	0%	0%	0%	0%	3%	3%	3%	3%	17%	3%	3%	3%	3%	10%
34	**34_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%	0%	0%	0%	0%	7%
35	**35_1**	0%	0%	0%	0%	0%	0%	0%	0%	3%	13%	0%	0%	3%	13%	13%
36	**36_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%
37	**37_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	10%	0%	0%	0%	0%	10%
38	**38_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
39	**39_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	10%
40	**40_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	7%



(a)



(b)

Figure 4.12 False rejection rate of different images for various thresholds with learning image size 50×50

(a) Rotation only (b) Rotation and translation

Table 4.4 Consolidated false rejection rate for learning image size 200×200

Threshold	Translation only		Rotation only		Translation plus rotation		Total falsely rejected images (out of 3600)	Overall FRR
	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR		
700	0	0.00%	62	5.17%	68	5.67%	130	3.61%
750	0	0.00%	79	6.58%	88	7.33%	167	4.64%
800	0	0.00%	125	10.42%	134	11.17%	259	7.19%
850	0	0.00%	200	16.67%	223	18.58%	423	11.75%
900	0	0.00%	369	30.75%	398	33.17%	767	21.31%

Table 4.5 Consolidated false rejection rate for learning image size 100×100

Threshold	Translation only		Rotation only		Translation plus rotation		Total falsely rejected images (out of 3600)	Overall FRR
	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR		
700	0	0.00%	14	1.17%	20	1.67%	34	0.94%
750	0	0.00%	20	1.67%	28	2.33%	48	1.33%
800	0	0.00%	48	4.00%	60	5.00%	108	3.00%
850	0	0.00%	100	8.33%	120	10.00%	220	6.11%
900	0	0.00%	250	20.83%	269	22.42%	519	14.42%

Table 4.6 Consolidated false rejection rate for learning image size 50×50

Threshold	Translation only		Rotation only		Translation plus rotation		Total falsely rejected images (out of 3600)	Overall FRR
	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR		
700	0	0.00%	1	0.08%	3	0.25%	4	0.11%
750	0	0.00%	3	0.25%	6	0.50%	9	0.25%
800	0	0.00%	9	0.75%	15	1.25%	24	0.67%
850	0	0.00%	23	1.92%	37	3.08%	60	1.67%
900	0	0.00%	82	6.83%	97	8.08%	179	4.97%

4.6.2 False Acceptance Rate (FAR)

False acceptance rate also known as false match rate (FMR) is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. False acceptance typically is considered the most serious of biometric security errors as it gives unauthorized users access to systems that expressly are trying to keep them out.

Each fingerprint image of different person in the database is compared with 100 images of the different person to find out the false match rate (FMR). The simulation results obtained for learning image sizes of 200×200, 100×100 and 50×50 have been tabulated in Table 4.7. No false acceptance has been found for the learning image size of 100×100 and 200×200 pixels upto a threshold of 700, however for learning image size of 50×50 pixels some false acceptance results have been observed. Figure 4.13 shows the graphical representation of the obtained results for learning image size 50×50. Table 4.8, shows the consolidated results of all the fingers in the database for learning image 50×50.

Table 4.7 False acceptance rate of different learning images and different thresholds

		Learning image size 200 × 200					Learning image size 100 × 100					Learning image size 50 × 50				
Sr. No.	**Image No.**	**Threshold**					**Threshold**					**Threshold**				
		700	**750**	**800**	**850**	**900**	**700**	**750**	**800**	**850**	**900**	**700**	**750**	**800**	**850**	**900**
1	**1_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
2	**2_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	25%	10%	5%	0%	0%
3	**3_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	40%	35%	30%	13%	0%
4	**4_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	50%	30%	5%	3%	0%
5	**5_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%
6	**6_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	28%	20%	13%	8%	0%
7	**7_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	50%	40%	10%	5%	5%
8	**8_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	4%	0%	0%	0%	0%
9	**9_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	5%	0%	0%	0%	0%
10	**10_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	45%	38%	23%	10%	0%
11	**11_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	28%	15%	10%	5%	3%
12	**12_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	40%	30%	20%	10%	5%
13	**13_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	13%	8%	8%	0%	0%
14	**14_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	5%	0%	0%	0%	0%
15	**15_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	23%	3%	0%	0%	0%
16	**16_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
17	**17_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	48%	30%	15%	3%	3%
18	**18_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
19	**19_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	63%	50%	23%	15%	5%
20	**20_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
21	**21_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	50%	23%	10%	5%	0%
22	**22_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
23	**23_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	53%	25%	15%	3%	0%
24	**24_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	40%	30%	20%	10%	5%
25	**25_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
26	**26_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	18%	10%	0%	0%	0%
27	**27_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
28	**28_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	5%	3%	0%	0%	0%
29	**29_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
30	**30_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%
31	**31_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	70%	55%	38%	15%	5%
32	**32_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	8%	0%	0%	0%	0%
33	**33_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	10%	0%	0%	0%	0%
34	**34_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	5%	0%	0%	0%	0%
35	**35_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
36	**36_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	43%	30%	18%	10%	3%
37	**37_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	20%	3%	0%	0%	0%
38	**38_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
39	**39_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
40	**40_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

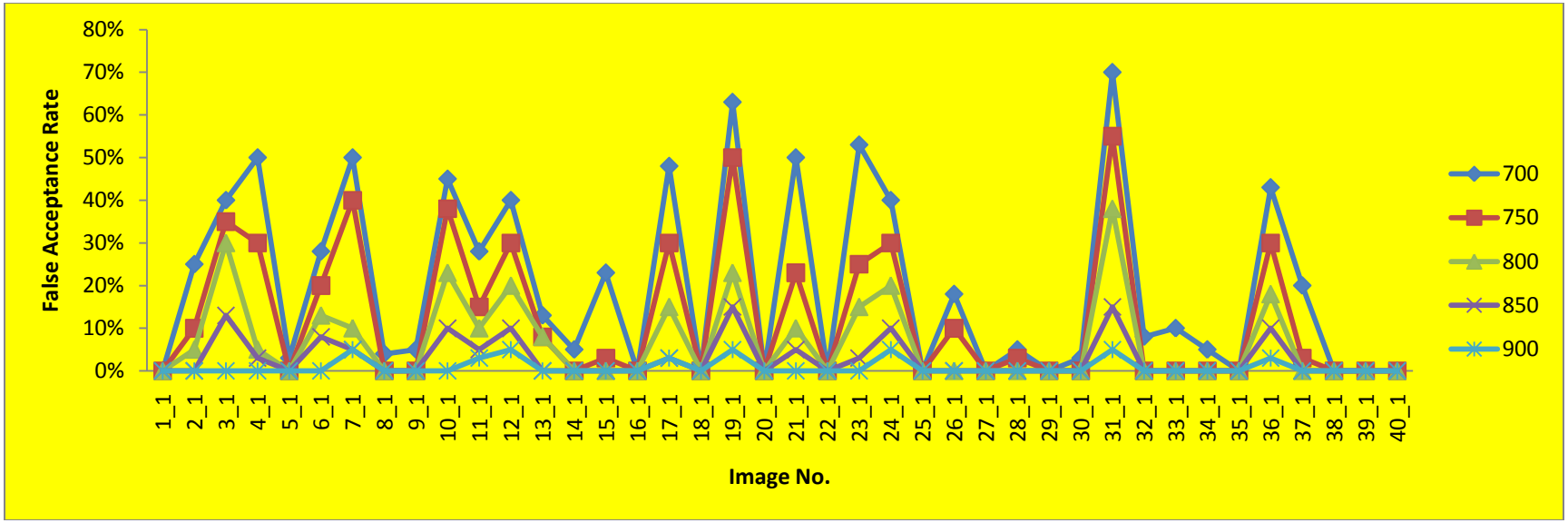


Figure 4.13 False acceptance rate of learning image size 50 × 50

Table 4.8 Consolidated false acceptance rate of different learning images and different thresholds

Threshold	Learning image size 200 × 200		Learning image size 100 × 100		Learning image size 50 × 50	
	Total falsely accepted images out of 4000	FAR	Total falsely accepted images out of 4000	FAR	Total falsely accepted images out of 4000	FAR
700	0	0%	0	0%	795	19.87%
750	0	0%	0	0%	488	12.20%
800	0	0%	0	0%	263	6.57%
850	0	0%	0	0%	115	2.875%
900	0	0%	0	0%	34	0.85%

4.7 Fingerprint Image Enhancement

In this section the effect of enhancement of the fingerprint images on the performance of the image based fingerprint verification system has been studied. Enhancement of the fingerprint image is required to be performed before the feature extraction stage as shown in Figure 4.14.

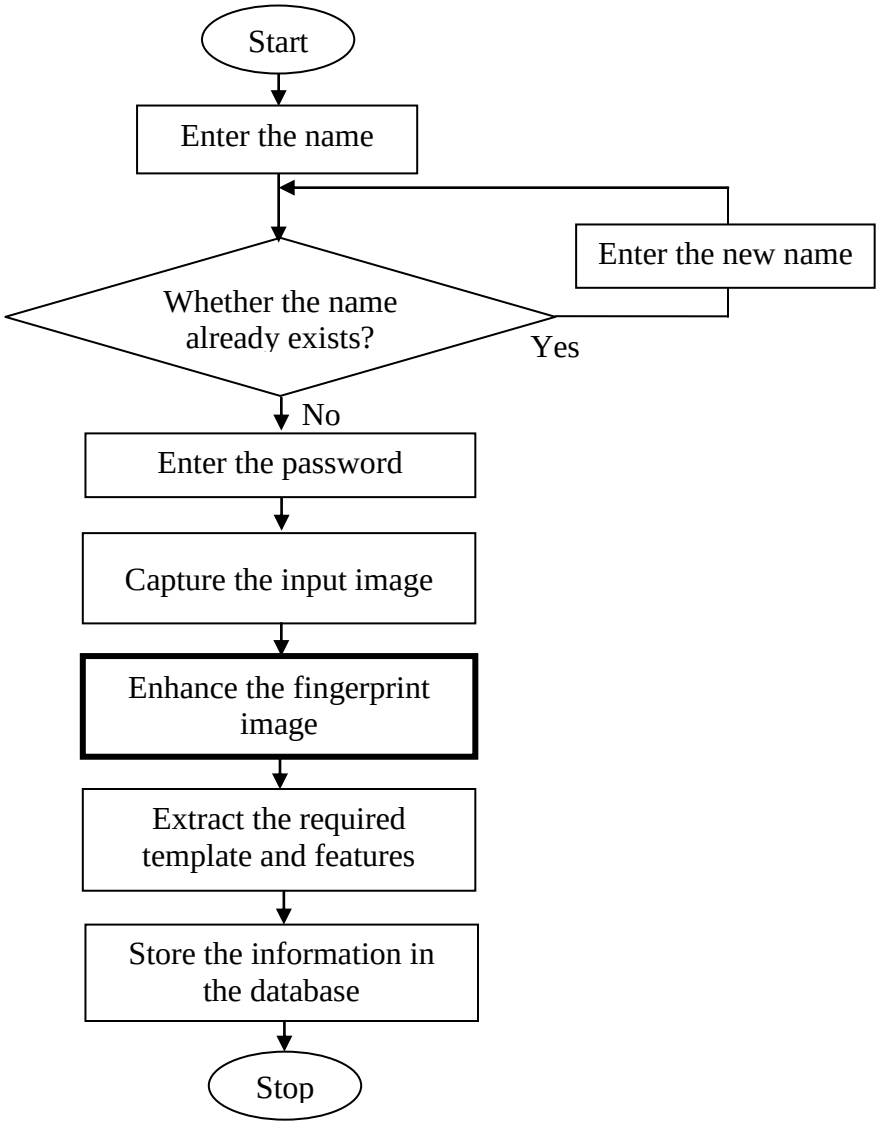


Figure 4.14 Flowchart of enrollment process with enhancement

Various fingerprint enhancement techniques have been discussed in the chapter 2 [69-77]. To have the contextual filtering in frequency domain the filter used should be separable in radial and angular domains [69]. The radial filter depends upon local ridge frequency

while the angular filter requires local ridge orientation and angular coherence. Moreover, due to the non stationary nature of the fingerprint image the traditional Fourier analysis is not adequate to analyze the image completely. Since the characteristics of the image are to be analyzed both in time and frequency so the image has to be divided into frames. Short Time Fourier Transform (STFT) analysis can fulfill both these requirements i.e. finding the local ridge frequency, local ridge orientation, angular coherence parameters and analyzing the fingerprint image into small frames.

The STFT based enhancement algorithm has the following advantages [75]:

(i) All the parameters of enhancement i.e. ridge orientation, ridge frequency, angular coherence etc. are probabilistically estimated simultaneously from STFT analysis.

(ii) The enhancement utilizes the full contextual information (ridge orientation, ridge frequency, angular coherence) for enhancement.

(iii) The algorithm has reduced space requirements compared to more popular Fourier domain based filtering techniques.

Chikkerur et al. [75] proposed a STFT based enhancement algorithm in which for STFT analysis, the image is divided overlapping windows (overlapping is done to preserve the ridge continuity). For each small region the probabilistic estimates of the ridge frequency, probabilistic estimates of the ridge orientation, angular coherence and region mask have been obtained using the STFT analysis.

STFT of a non-stationary 1D signal $x(t)$ and window , $X(\tau, \omega)$ [176] is given by

X (τ, ω) (4.2)

and STFT of a non-stationary 2D signal is given by

(4.3)

Here represent the spatial positions and ω_1, ω_2 represents the spatial frequency parameters of the two dimensional Hanning window . Any local region in the fingerprint image has a consistent orientation (except at singular points such as core and delta). Therefore, the local region can be approximated as a surface wave that is characterized completely by its orientation θ and frequency f. If θ is a random variable with probability density function $p(\theta)$. The expected value of the orientation may then be obtained by performing a vector averaging

(4.4)

However, ridge orientation can be estimated by considering the orientation of its immediate neighborhood if there is a crease in the fingerprints that spans several analysis frames or when the frame consists entirely of unrecoverable regions with poor ridge structure or poor ridge contrast. The resulting orientation image is further smoothened using vectorial averaging. The smoothened image is obtained by using

(4.5)

represents a 3x3 Gaussian smoothening kernel.

The orientation image is used to compute the angular coherence [177]. The coherence is related to dispersion measure of the circular data and is given by

(4.6)

The coherence is high when the orientation of the central block is similar to each of its neighbors . In a fingerprint image, the coherence is low close to the points of the singularity. If ridge frequency to be a random variable with the probability density function $p(r)$ then the expected value of the ridge frequency is given by

(4.7)

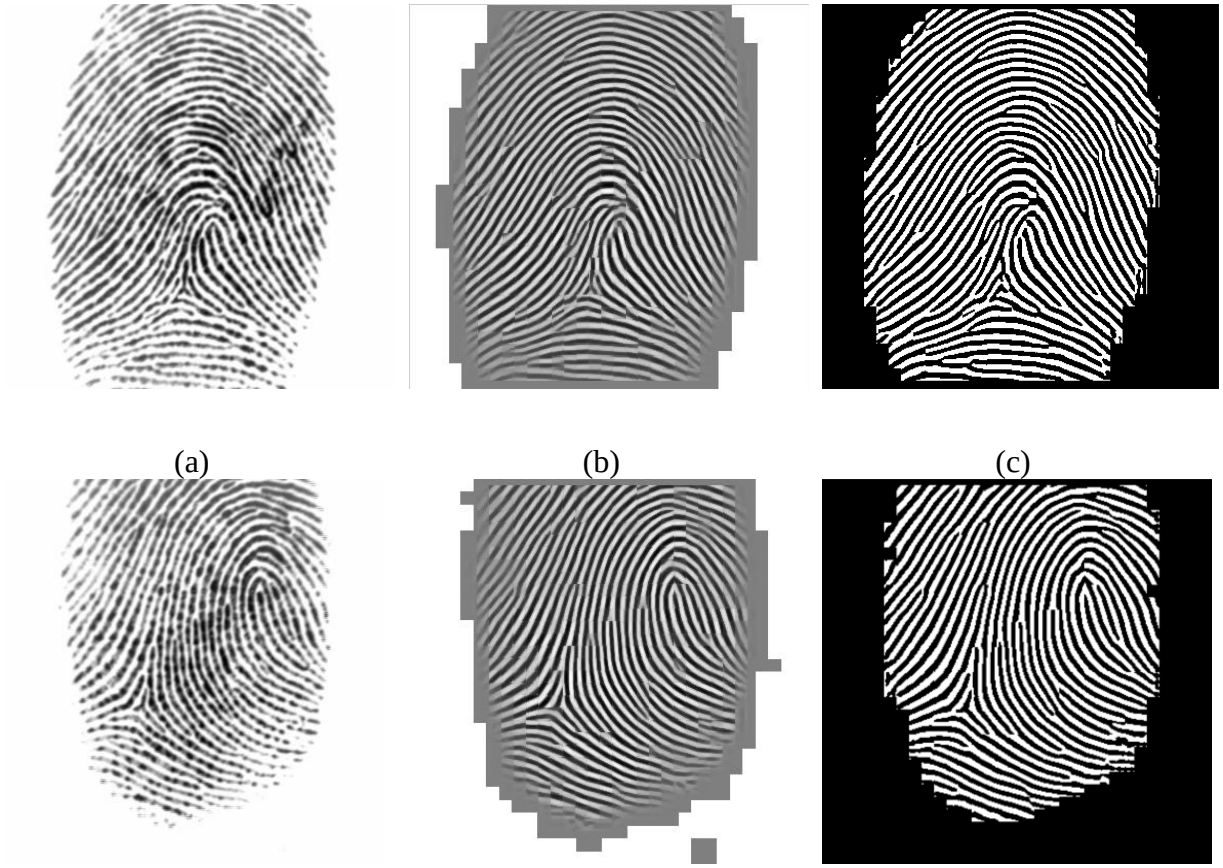
The frequency map so obtained is smoothened by process of isotropic diffusion [70] and is given by:

(4.8)

The variable ensures that only valid ridge frequencies are considered during the smoothening process. is non zero only if the ridge frequency is within the valid range otherwise it will assume a zero value.

The information obtained in STFT analysis is used to compute the radial and angular filters. The angular filters are calculated by having the information of mean angle from the orientation image and angular bandwidth from the coherence image, centered around
The radial filter is calculated from the ridge frequency and centered around . These filters are used to filter each block in the Fourier domain. The enhanced block is obtained by performing the inverse Fourier transform. This process is repeated for all the blocks and the

enhanced image is obtained by tiling the result of each enhanced block. This work presents the modified version of the algorithm proposed by Chikkerur et al. [75]. Instead of performing the STFT analysis of all the blocks and then cleaning the resulting image with region mask, STFT analysis of only those blocks have been calculated which have the variance value greater than a particular value. Results obtained by Chikkerur et al. [75] algorithm and modified STFT enhancement algorithm as proposed in the present work, have been shown in Figure 4.15 for the images 1_1 and 2_1 from database FVC2002/Db1_a. As shown in the Figure 4.15 it can be concluded that the results obtained by the modified STFT algorithm are far better than the results obtained by original STFT enhancement algorithm.

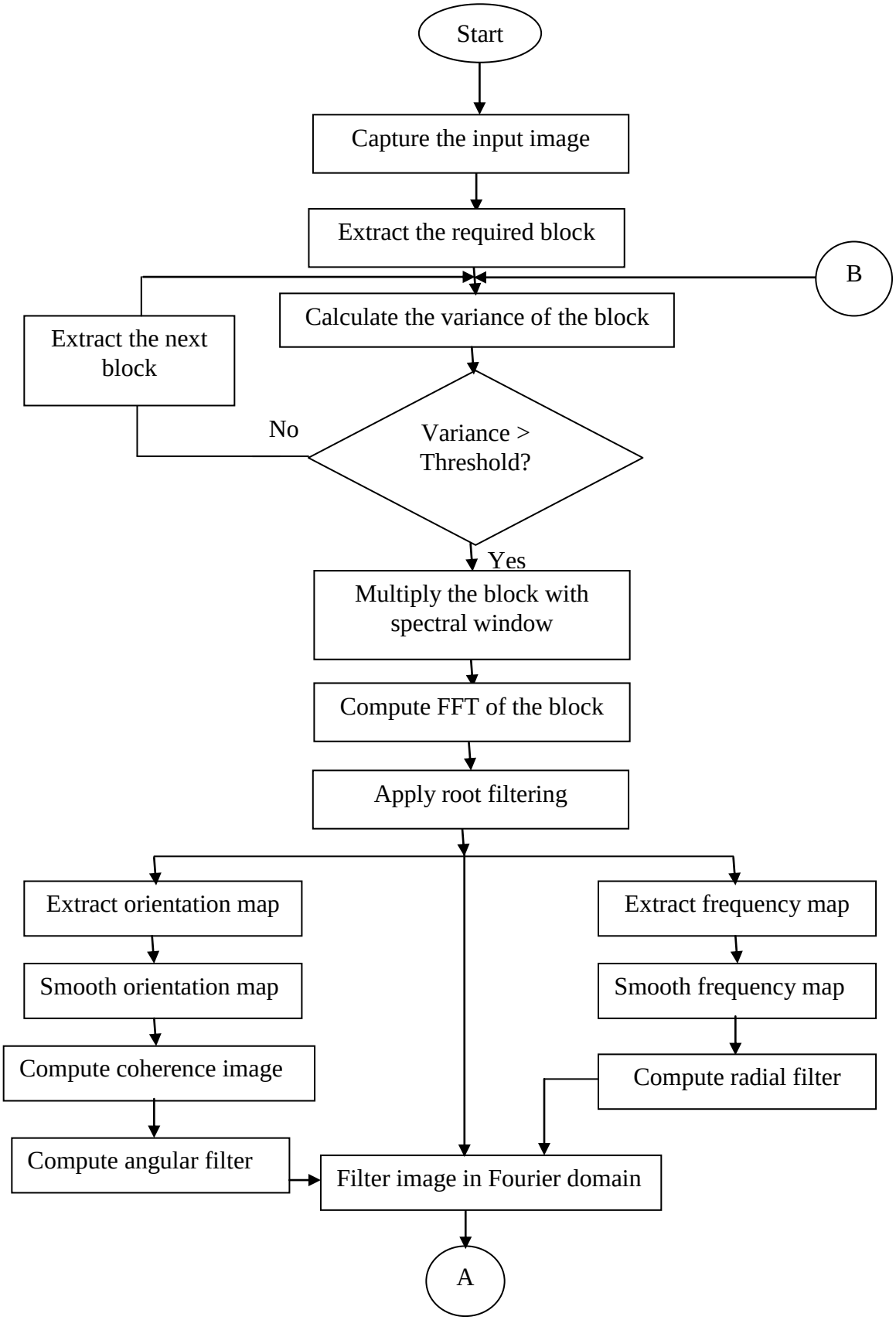


(a) (b) (c)

(d) (e) (f)

Figure 4.15 (a) Original 1_1 image (b) Enhanced 1_1 image by Chikkerur et al. method (c) Enhanced 1_1 image by proposed method (d) Original 2_1 image (e) Enhanced 2_1 image by Chikkerur et al. method (f) Enhanced 2_1 image by proposed method

The flow chart of the enhancement process is shown in Figure 4.16.



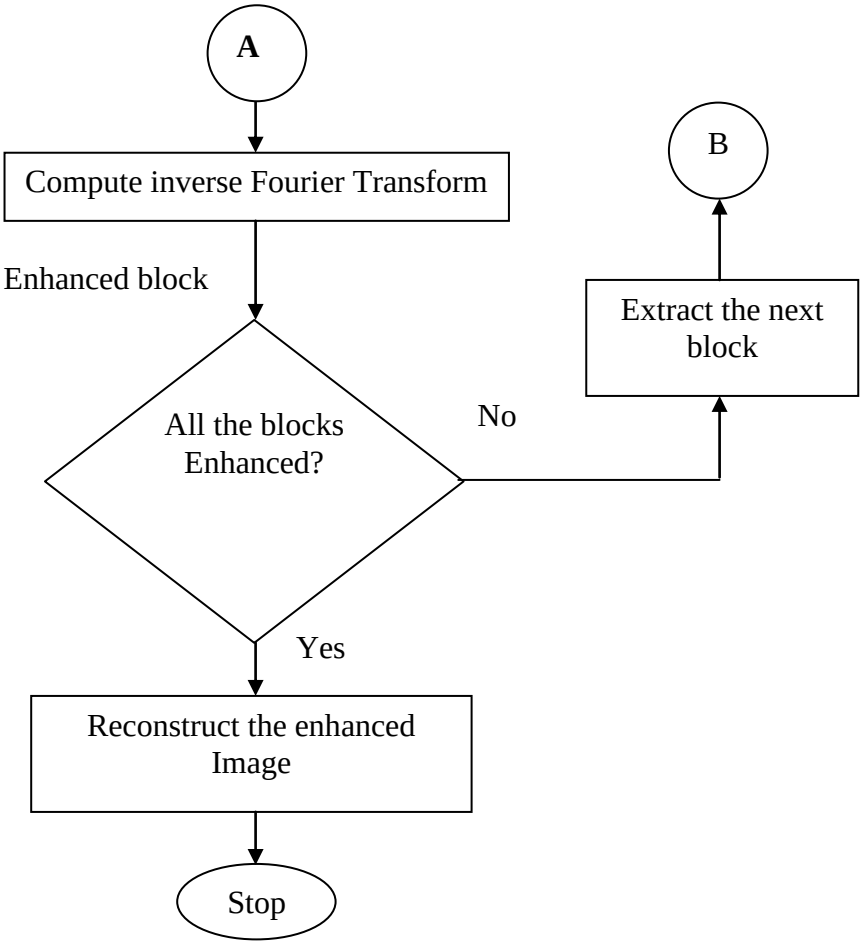


Figure 4.16 Flow chart of the enhancement algorithm

4.8 Database and Results of Enhanced Fingerprint Images

The fingerprint images of database FVC2002/Db1_a have been enhanced using the method discussed in section 4.7 and database has been created in the similar manner by translating, rotating and translating plus rotating the enhanced images as explained in section 4.5. The images of template size of 50×50, 100×100 and 200×200 pixels have also been extracted in the same manner and from the same positions as that of the original database. Figure 4.17 shows the enhanced extracted images of template size 50×50, 100×100 and 200×200 pixels respectively from the enhanced image 1_1 of FVC2002/Db1_a database.

(a) (b) (c)

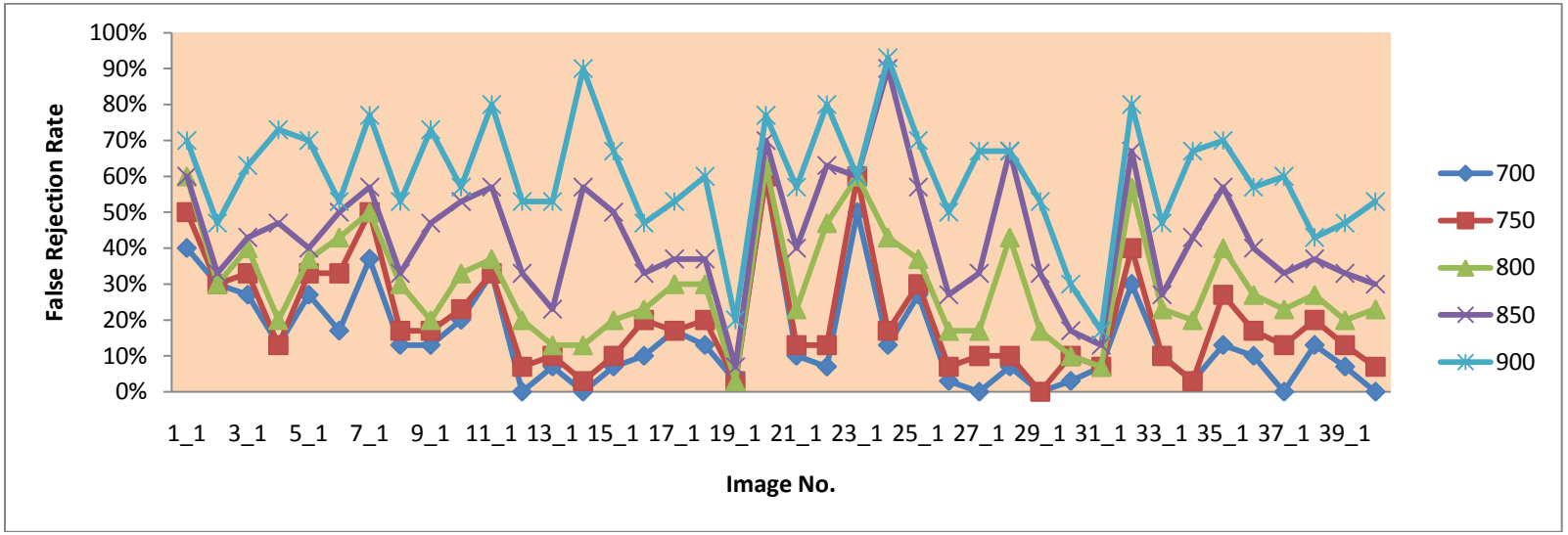
Figure 4.17 Template size of (a) 50×50 pixels (b) 100×100 pixels (c) 200×200 pixels extracted from enhanced image 1_1 of FVC2002/Db1_a database

The simulation results obtained for learning image sizes of 200×200, 100×100 and 50×50 have been tabulated in Table 4.9, Table 4.10 and Table 4.11 respectively. Figure 4.18, Figure 4.19 and Figure 4.20 shows the graphical representation of the obtained results. Table 4.12, Table 4.13 and Table 4.14 shows the consolidated results of all the fingerprints in the database for learning image sizes of 200×200, 100×100 and 50×50 respectively.

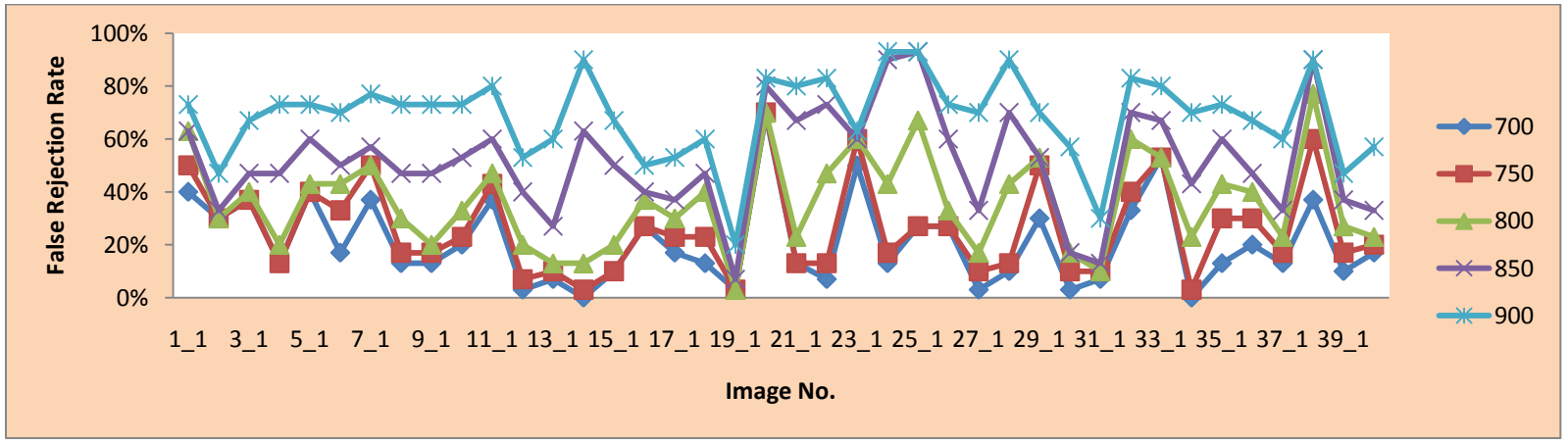
Table 4.15 represents the false acceptance rate results obtained for different sized learning images. Figure 4.21shows the graphical representation of the obtained FAR results for 50×50 size learning image while Table 4.16 represents the consolidated FAR results.

Table 4.9 False rejection rate of enhanced images for learning image size 200× 200

Sr. No.	Image No.	Translated					Rotated					Translated plus rotated				
		Threshold					Threshold					Threshold				
		700	750	800	850	900	700	750	800	850	900	700	750	800	850	900
1	1_1	0%	0%	0%	0%	0%	40%	50%	60%	60%	70%	40%	50%	63%	63%	73%
2	2_1	0%	0%	0%	0%	0%	30%	30%	30%	33%	47%	30%	30%	30%	33%	47%
3	3_1	0%	0%	0%	0%	0%	27%	33%	40%	43%	63%	37%	37%	40%	47%	67%
4	4_1	0%	0%	0%	0%	0%	13%	13%	20%	47%	73%	13%	13%	20%	47%	73%
5	5_1	0%	0%	0%	0%	0%	27%	33%	37%	40%	70%	40%	40%	43%	60%	73%
6	6_1	0%	0%	0%	0%	0%	17%	33%	43%	50%	53%	17%	33%	43%	50%	70%
7	7_1	0%	0%	0%	0%	0%	37%	50%	50%	57%	77%	37%	50%	50%	57%	77%
8	8_1	0%	0%	0%	0%	0%	13%	17%	30%	33%	53%	13%	17%	30%	47%	73%
9	9_1	0%	0%	0%	0%	0%	13%	17%	20%	47%	73%	13%	17%	20%	47%	73%
10	10_1	0%	0%	0%	0%	0%	20%	23%	33%	53%	57%	20%	23%	33%	53%	73%
11	11_1	0%	0%	0%	0%	0%	33%	33%	37%	57%	80%	37%	43%	47%	60%	80%
12	12_1	0%	0%	0%	0%	0%	0%	7%	20%	33%	53%	3%	7%	20%	40%	53%
13	13_1	0%	0%	0%	0%	0%	7%	10%	13%	23%	53%	7%	10%	13%	27%	60%
14	14_1	0%	0%	0%	0%	0%	0%	3%	13%	57%	90%	0%	3%	13%	63%	90%
15	15_1	0%	0%	0%	0%	0%	7%	10%	20%	50%	67%	10%	10%	20%	50%	67%
16	16_1	0%	0%	0%	0%	0%	10%	20%	23%	33%	47%	27%	27%	37%	40%	50%
17	17_1	0%	0%	0%	0%	0%	17%	17%	30%	37%	53%	17%	23%	30%	37%	53%
18	18_1	0%	0%	0%	0%	0%	13%	20%	30%	37%	60%	13%	23%	40%	47%	60%
19	19_1	0%	0%	0%	0%	0%	3%	3%	3%	7%	20%	3%	3%	3%	7%	20%
20	20_1	0%	0%	0%	0%	0%	60%	60%	63%	70%	77%	69%	70%	70%	80%	83%
21	21_1	0%	0%	0%	0%	0%	10%	13%	23%	40%	57%	13%	13%	23%	67%	80%
22	22_1	0%	0%	0%	0%	0%	7%	13%	47%	63%	80%	7%	13%	47%	73%	83%
23	23_1	0%	0%	0%	0%	0%	50%	60%	60%	60%	60%	50%	60%	60%	60%	63%
24	24_1	0%	0%	0%	0%	0%	13%	17%	43%	90%	93%	13%	17%	43%	90%	93%
25	25_1	0%	0%	0%	0%	0%	27%	30%	37%	57%	70%	27%	27%	67%	93%	93%
26	26_1	0%	0%	0%	0%	0%	3%	7%	17%	27%	50%	27%	27%	33%	60%	73%
27	27_1	0%	0%	0%	0%	0%	0%	10%	17%	33%	67%	3%	10%	17%	33%	70%
28	28_1	0%	0%	0%	0%	0%	7%	10%	43%	67%	67%	10%	13%	43%	70%	90%
29	29_1	0%	0%	0%	0%	0%	0%	0%	17%	33%	53%	30%	50%	53%	53%	70%
30	30_1	0%	0%	0%	0%	0%	3%	10%	10%	17%	30%	3%	10%	17%	17%	57%
31	31_1	0%	0%	0%	0%	0%	7%	7%	7%	13%	17%	7%	10%	10%	13%	30%
32	32_1	0%	0%	0%	0%	0%	30%	40%	57%	67%	80%	33%	40%	60%	70%	83%
33	33_1	0%	0%	0%	0%	0%	10%	10%	23%	27%	47%	53%	53%	53%	67%	80%
34	34_1	0%	0%	0%	0%	0%	3%	3%	20%	43%	67%	0%	3%	23%	43%	70%
35	35_1	0%	0%	0%	0%	0%	13%	27%	40%	57%	70%	13%	30%	43%	60%	73%
36	36_1	0%	0%	0%	0%	0%	10%	17%	27%	40%	57%	20%	30%	40%	47%	67%
37	37_1	0%	0%	0%	0%	0%	0%	13%	23%	33%	60%	13%	17%	23%	33%	60%
38	38_1	0%	0%	0%	0%	0%	13%	20%	27%	37%	43%	37%	60%	77%	90%	90%
39	39_1	0%	0%	0%	0%	0%	7%	13%	20%	33%	47%	10%	17%	27%	37%	47%
40	40_1	0%	0%	0%	0%	0%	0%	7%	23%	30%	53%	17%	20%	23%	33%	57%



(a)



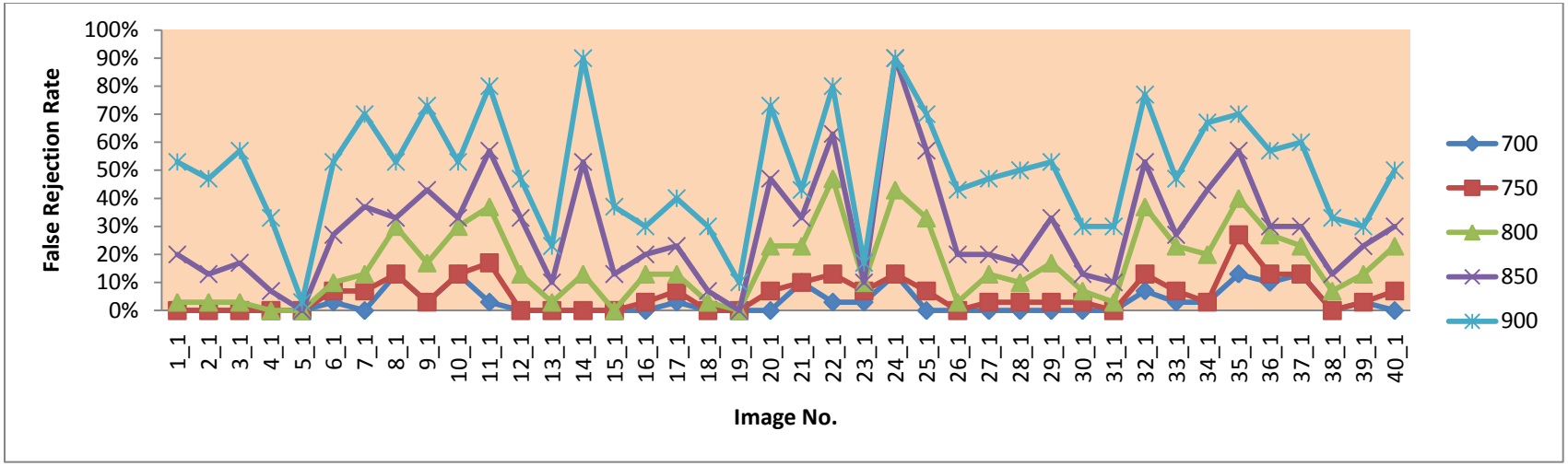
(b)

Figure 4.18 False rejection rate of different enhanced images for various thresholds with learning image size 200× 200

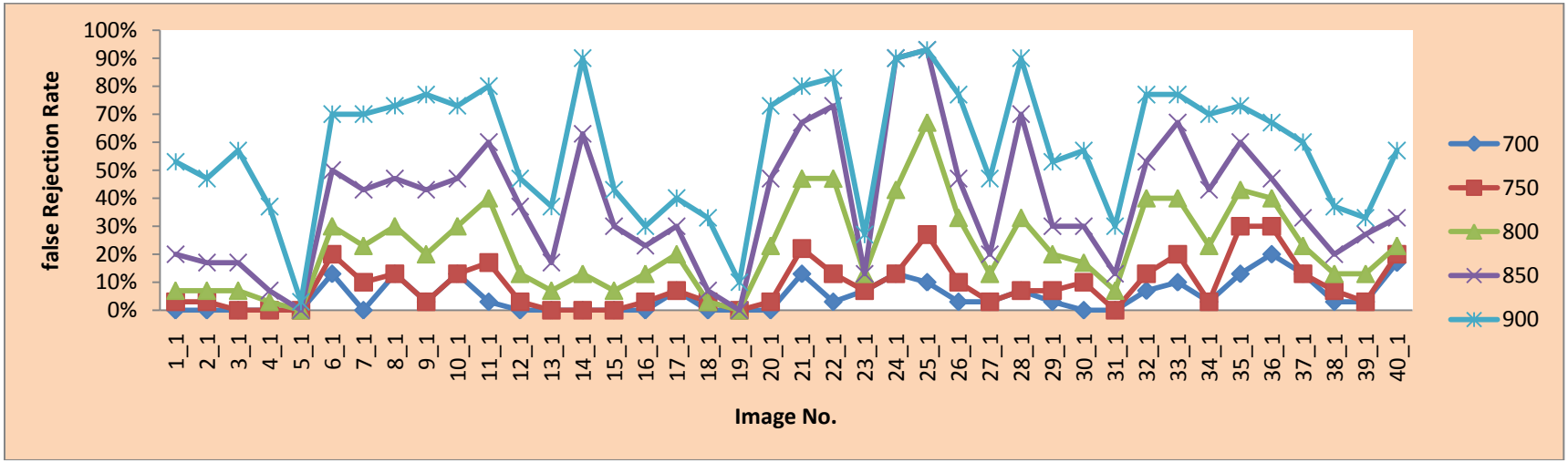
(a) Rotation only (b) Rotation and translation

Table 4.10 False rejection rate of enhanced images for learning image size 100×100

Sr. No.	Image No.	Translated					Rotated					Translated plus rotated				
		Threshold					Threshold					Threshold				
		700	750	800	850	900	700	750	800	850	900	700	750	800	850	900
1	**1_1**	0%	0%	0%	0%	0%	0%	0%	3%	20%	53%	0%	3%	7%	20%	53%
2	**2_1**	0%	0%	0%	0%	0%	0%	0%	3%	13%	47%	0%	3%	7%	17%	47%
3	**3_1**	0%	0%	0%	0%	0%	0%	0%	3%	17%	57%	0%	0%	7%	17%	57%
4	**4_1**	0%	0%	0%	0%	0%	0%	0%	0%	7%	33%	0%	0%	3%	7%	37%
5	**5_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	3%
6	**6_1**	0%	0%	0%	0%	0%	3%	7%	10%	27%	53%	13%	20%	30%	50%	70%
7	**7_1**	0%	0%	0%	0%	0%	0%	7%	13%	37%	70%	0%	10%	23%	43%	70%
8	**8_1**	0%	0%	0%	0%	0%	13%	13%	30%	33%	53%	13%	13%	30%	47%	73%
9	**9_1**	0%	0%	0%	0%	0%	3%	3%	17%	43%	73%	3%	3%	20%	43%	77%
10	**10_1**	0%	0%	0%	0%	0%	13%	13%	30%	33%	53%	13%	13%	30%	47%	73%
11	**11_1**	0%	0%	0%	0%	0%	3%	17%	37%	57%	80%	3%	17%	40%	60%	80%
12	**12_1**	0%	0%	0%	0%	0%	0%	0%	13%	33%	47%	0%	3%	13%	37%	47%
13	**13_1**	0%	0%	0%	0%	0%	0%	0%	3%	10%	23%	0%	0%	7%	17%	37%
14	**14_1**	0%	0%	0%	0%	0%	0%	0%	13%	53%	90%	0%	0%	13%	63%	90%
15	**15_1**	0%	0%	0%	0%	0%	0%	0%	0%	13%	37%	0%	0%	7%	30%	43%
16	**16_1**	0%	0%	0%	0%	0%	0%	3%	13%	20%	30%	0%	3%	13%	23%	30%
17	**17_1**	0%	0%	0%	0%	0%	3%	7%	13%	23%	40%	7%	7%	20%	30%	40%
18	**18_1**	0%	0%	0%	0%	0%	0%	0%	3%	7%	30%	0%	3%	3%	7%	33%
19	**19_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	10%	0%	0%	0%	0%	10%
20	**20_1**	0%	0%	0%	0%	0%	0%	7%	23%	47%	73%	0%	3%	23%	47%	73%
21	**21_1**	0%	0%	0%	0%	0%	10%	10%	23%	33%	43%	13%	22%	47%	67%	80%
22	**22_1**	0%	0%	0%	0%	0%	3%	13%	47%	63%	80%	3%	13%	47%	73%	83%
23	**23_1**	0%	0%	0%	0%	0%	3%	7%	10%	10%	17%	7%	7%	13%	13%	27%
24	**24_1**	0%	0%	0%	0%	0%	13%	13%	43%	90%	90%	13%	13%	43%	90%	90%
25	**25_1**	0%	0%	0%	0%	0%	0%	7%	33%	57%	70%	10%	27%	67%	93%	93%
26	**26_1**	0%	0%	0%	0%	0%	0%	0%	3%	20%	43%	3%	10%	33%	47%	77%
27	**27_1**	0%	0%	0%	0%	0%	0%	3%	13%	20%	47%	3%	3%	13%	20%	47%
28	**28_1**	0%	0%	0%	0%	0%	0%	3%	10%	17%	50%	7%	7%	33%	70%	90%
29	**29_1**	0%	0%	0%	0%	0%	0%	3%	17%	33%	53%	3%	7%	20%	30%	53%
30	**30_1**	0%	0%	0%	0%	0%	0%	3%	7%	13%	30%	0%	10%	17%	30%	57%
31	**31_1**	0%	0%	0%	0%	0%	0%	0%	3%	10%	30%	0%	0%	7%	13%	30%
32	**32_1**	0%	0%	0%	0%	0%	7%	13%	37%	53%	77%	7%	13%	40%	53%	77%
33	**33_1**	0%	0%	0%	0%	0%	3%	7%	23%	27%	47%	10%	20%	40%	67%	77%
34	**34_1**	0%	0%	0%	0%	0%	3%	3%	20%	43%	67%	3%	3%	23%	43%	70%
35	**35_1**	0%	0%	0%	0%	0%	13%	27%	40%	57%	70%	13%	30%	43%	60%	73%
36	**36_1**	0%	0%	0%	0%	0%	10%	13%	27%	30%	57%	20%	30%	40%	47%	67%
37	**37_1**	0%	0%	0%	0%	0%	13%	13%	23%	30%	60%	13%	13%	23%	33%	60%
38	**38_1**	0%	0%	0%	0%	0%	0%	0%	7%	13%	33%	3%	7%	13%	20%	37%
39	**39_1**	0%	0%	0%	0%	0%	3%	3%	13%	23%	30%	3%	3%	13%	27%	33%
40	**40_1**	0%	0%	0%	0%	0%	0%	7%	23%	30%	50%	17%	20%	23%	33%	57%



(a)



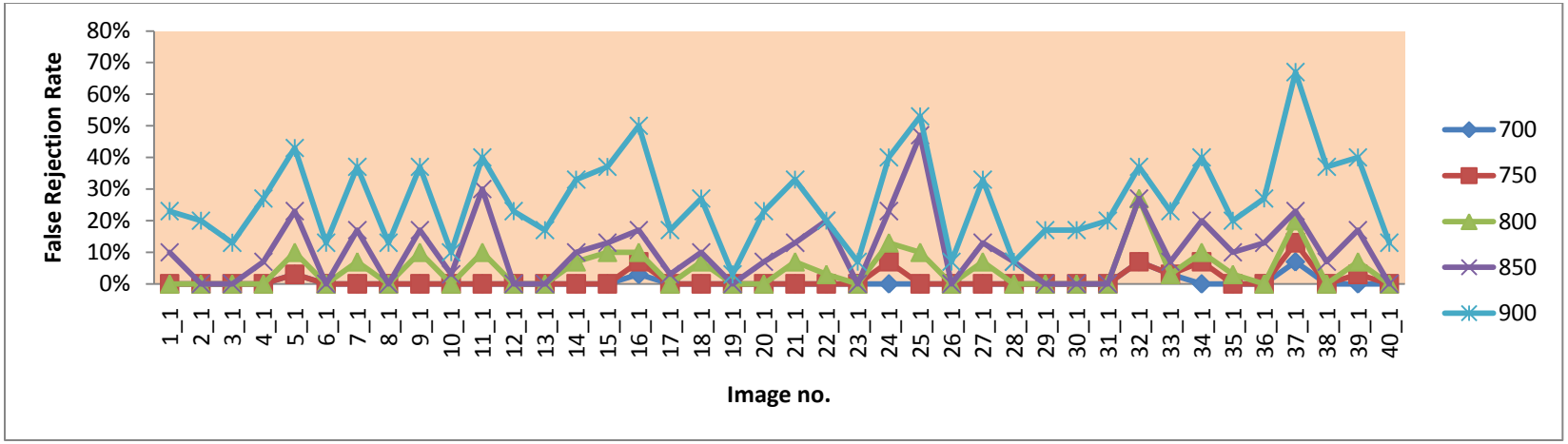
(b)

Figure 4.19 False rejection rate of different enhanced images for various thresholds with learning image size 100× 100

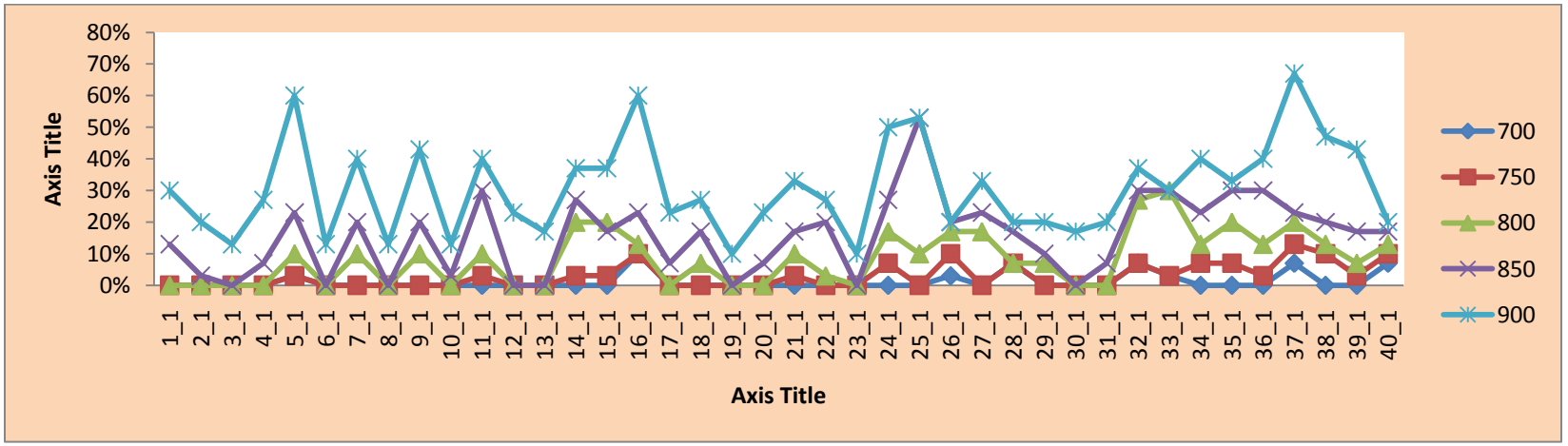
(a) Rotation only (b) Rotation and translation

Table 4.11 False rejection rate of enhanced images for learning image size 50×50

Sr. No.	Image No.	Translated					Rotated					Translated plus rotated				
		Threshold					Threshold					Threshold				
		700	750	800	850	900	700	750	800	850	900	700	750	800	850	900
1	**1_1**	0%	0%	0%	0%	0%	0%	0%	0%	10%	23%	0%	0%	0%	13%	30%
2	**2_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	20%	0%	0%	0%	3%	20%
3	**3_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	13%	0%	0%	0%	0%	13%
4	**4_1**	0%	0%	0%	0%	0%	0%	0%	0%	7%	27%	0%	0%	0%	7%	27%
5	**5_1**	0%	0%	0%	0%	0%	3%	3%	10%	23%	43%	3%	3%	10%	23%	60%
6	**6_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	13%	0%	0%	0%	0%	13%
7	**7_1**	0%	0%	0%	0%	0%	0%	0%	7%	17%	37%	0%	0%	10%	20%	40%
8	**8_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	13%	0%	0%	0%	0%	13%
9	**9_1**	0%	0%	0%	0%	0%	0%	0%	10%	17%	37%	0%	0%	10%	20%	43%
10	**10_1**	0%	0%	0%	0%	0%	0%	0%	0%	3%	10%	0%	0%	0%	3%	13%
11	**11_1**	0%	0%	0%	0%	0%	0%	0%	10%	30%	40%	0%	3%	10%	30%	40%
12	**12_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	23%	0%	0%	0%	0%	23%
13	**13_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	17%	0%	0%	0%	0%	17%
14	**14_1**	0%	0%	0%	0%	0%	0%	0%	7%	10%	33%	0%	3%	20%	27%	37%
15	**15_1**	0%	0%	0%	0%	0%	0%	0%	10%	13%	37%	0%	3%	20%	17%	37%
16	**16_1**	0%	0%	0%	0%	0%	3%	7%	10%	17%	50%	10%	10%	13%	23%	60%
17	**17_1**	0%	0%	0%	0%	0%	0%	0%	0%	3%	17%	0%	0%	0%	7%	23%
18	**18_1**	0%	0%	0%	0%	0%	0%	0%	7%	10%	27%	0%	0%	7%	17%	27%
19	**19_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%	10%
20	**20_1**	0%	0%	0%	0%	0%	0%	0%	0%	7%	23%	0%	0%	0%	7%	23%
21	**21_1**	0%	0%	0%	0%	0%	0%	0%	7%	13%	33%	0%	3%	10%	17%	33%
22	**22_1**	0%	0%	0%	0%	0%	0%	0%	3%	20%	20%	0%	0%	3%	20%	27%
23	**23_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%	0%	0%	0%	0%	10%
24	**24_1**	0%	0%	0%	0%	0%	0%	7%	13%	23%	40%	0%	7%	17%	27%	50%
25	**25_1**	0%	0%	0%	0%	0%	0%	0%	10%	47%	53%	0%	0%	10%	53%	53%
26	**26_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%	3%	10%	17%	20%	20%
27	**27_1**	0%	0%	0%	0%	0%	0%	0%	7%	13%	33%	0%	0%	17%	23%	33%
28	**28_1**	0%	0%	0%	0%	0%	0%	0%	0%	7%	7%	7%	7%	7%	17%	20%
29	**29_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	17%	0%	0%	7%	10%	20%
30	**30_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	17%	0%	0%	0%	0%	17%
31	**31_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	20%	0%	0%	0%	7%	20%
32	**32_1**	0%	0%	0%	0%	0%	7%	7%	27%	27%	37%	7%	7%	27%	30%	37%
33	**33_1**	0%	0%	0%	0%	0%	3%	3%	3%	7%	23%	3%	3%	30%	30%	30%
34	**34_1**	0%	0%	0%	0%	0%	0%	7%	10%	20%	40%	0%	7%	13%	23%	40%
35	**35_1**	0%	0%	0%	0%	0%	0%	0%	3%	10%	20%	0%	7%	20%	30%	33%
36	**36_1**	0%	0%	0%	0%	0%	0%	0%	0%	13%	27%	0%	3%	13%	30%	40%
37	**37_1**	0%	0%	0%	0%	0%	7%	13%	20%	23%	67%	7%	13%	20%	23%	67%
38	**38_1**	0%	0%	0%	0%	0%	0%	0%	0%	7%	37%	0%	10%	13%	20%	47%
39	**39_1**	0%	0%	0%	0%	0%	0%	3%	7%	17%	40%	0%	3%	7%	17%	43%
40	**40_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	13%	7%	10%	13%	17%	20%



(a)



(b)

Figure 4.20 False rejection rate of different enhanced images for various thresholds with learning image size 50×50 (a) Rotation only (b) Rotation and translation

Table 4.12 Consolidated false rejection rate of enhanced fingerprint image for learning image size 200×200

Threshold	**Translation only**		**Rotation only**		**Translation plus rotation**		Total falsely rejected images (out of 3600)	**Overall FRR**
	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR		
700	0	0%	180	15.00%	250	20.83%	430	11.94%
750	0	0%	243	20.25%	315	26.25%	558	15.50%
800	0	0%	359	29.92%	434	36.17%	793	22.03%
850	0	0%	520	43.33%	619	51.58%	1139	31.64%
900	0	0%	721	60.08%	823	68.58%	1544	42.89%

Table 4.13 Consolidated false rejection rate enhanced fingerprint image for learning image size 100×100

Threshold	**Translation only**		**Rotation only**		**Translation plus rotation**		Total falsely rejected images (out of 3600)	**Overall FRR**
	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR		
700	0	0%	36	3.00%	61	5.08%	97	2.69%
750	0	0%	68	5.67%	108	9.00%	176	4.89%
800	0	0%	195	16.25%	268	22.33%	463	12.86%
850	0	0%	350	29.17%	460	38.33%	810	22.50%
900	0	0%	600	50.00%	696	58.00%	1296	36.00%

Table 4.14 Consolidated false rejection rate enhanced fingerprint image for learning image size 50×50

Threshold	**Translation only**		**Rotation only**		**Translation plus rotation**		Total falsely rejected images (out of 3600)	**Overall FRR**
	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR	Falsely rejected images (out of 1200)	FRR		
700	0	0%	7	0.58%	14	1.17%	21	0.58%
750	0	0%	15	1.25%	34	2.83%	49	1.36%
800	0	0%	54	4.50%	103	8.58%	157	4.36%
850	0	0%	124	10.33%	189	15.75%	313	8.69%
900	0	0%	319	26.58%	369	30.75%	688	19.11%

Table 4.15 False acceptance rate of enhanced fingerprint images for different learning images and different thresholds

		Learning image size 200× 200					Learning image size 100× 100					Learning image size 50× 50				
Sr. No.	Image No.	Threshold					Threshold					Threshold				
		700	750	800	850	900	700	750	800	850	900	700	750	800	850	900
1	**1_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
2	**2_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	25%	12%	5%	3%	2%
3	**3_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	44%	35%	33%	13%	0%
4	**4_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	50%	30%	5%	3%	0%
5	**5_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	8%	0%	0%	0%	0%
6	**6_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	20%	13%	5%	0%	0%
7	**7_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	53%	40%	23%	10%	5%
8	**8_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	8%	0%	0%	0%	0%
9	**9_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	5%	0%	0%	0%	0%
10	**10_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	63%	55%	38%	25%	0%
11	**11_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	30%	18%	13%	10%	5%
12	**12_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	40%	35%	22%	10%	5%
13	**13_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
14	**14_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%
15	**15_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	50%	38%	8%	0%	0%
16	**16_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
17	**17_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	40%	25%	20%	15%	0%
18	**18_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
19	**19_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	68%	65%	50%	35%	20%
20	**20_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
21	**21_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	73%	55%	30%	20%	3%
22	**22_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
23	**23_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	65%	50%	38%	18%	13%
24	**24_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	40%	35%	22%	10%	5%
25	**25_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	33%	25%	18%	5%	0%
26	**26_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	23%	10%	3%	0%	0%
27	**27_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%
28	**28_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%
29	**29_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	25%	15%	10%	3%	0%
30	**30_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	25%	15%	10%	3%	3%
31	**31_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	73%	70%	55%	28%	8%
32	**32_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	25%	13%	3%	0%	0%
33	**33_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	58%	40%	20%	3%	0%
34	**34_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	48%	20%	3%	0%	0%
35	**35_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	30%	8%	0%	0%	0%
36	**36_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	38%	28%	13%	10%	0%
37	**37_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	33%	23%	3%	0%	0%
38	**38_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	25%	15%	13%	3%	0%
39	**39_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	48%	13%	3%	0%	0%
40	**40_1**	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	0%

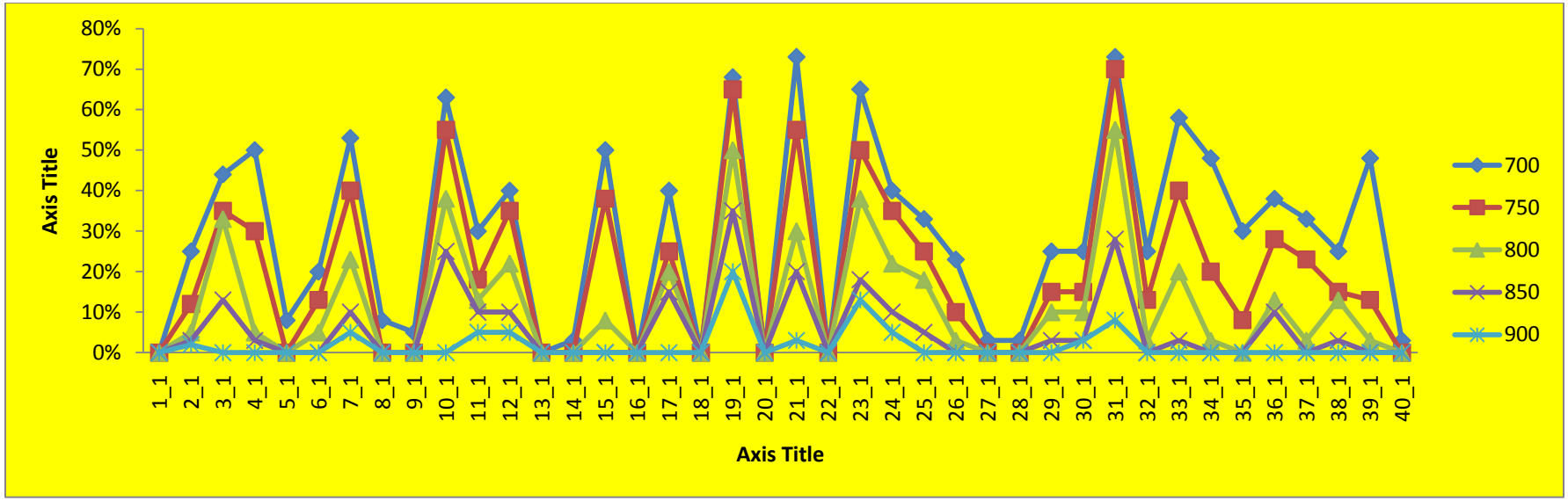


Figure 4.21 False acceptance rate of enhanced fingerprint images for learning image size 50×50

Table 4.16 Consolidated false acceptance rate of enhanced fingerprint images for different learning images and different thresholds

Threshold	**Learning image size 200×200**		**Learning image size 100×100**		**Learning image size 50×50**	
	Total falsely accepted images	FAR	Total falsely accepted images	FAR	Total falsely accepted images	FAR
700	0	0%	0	0%	1178	29.45%
750	0	0%	0	0%	801	20.025%
800	0	0%	0	0%	466	11.65%
850	0	0%	0	0%	227	5.675%
900	0	0%	0	0%	69	1.725%

4.9 Comparison of Results and Discussion

The Table 4.17 shows the false rejection rate for three different sized learning images (200×200, 100×100 and 50×50) at different thresholds for original and enhanced database while Figure 4.22 shows its graphical representation.

Table 4.17 Comparison of false rejection rate for different learning image sizes of original and enhanced database

Threshold	**Original database (FRR)**			**Enhanced database (FRR)**		
	Template size					
	200×200	**100×100**	**50×50**	**200×200**	**100×100**	**50×50**
700	3.61%	0.94%	0.11%	11.94%	2.69%	0.58%
750	4.64%	1.33%	0.25%	15.50%	4.89%	1.36%
800	7.19%	3.00%	0.67%	22.03%	12.86%	4.36%
850	11.75%	6.11%	1.67%	31.64%	22.50%	8.69%
900	21.31%	14.42%	4.97%	42.89%	36.00%	19.11%

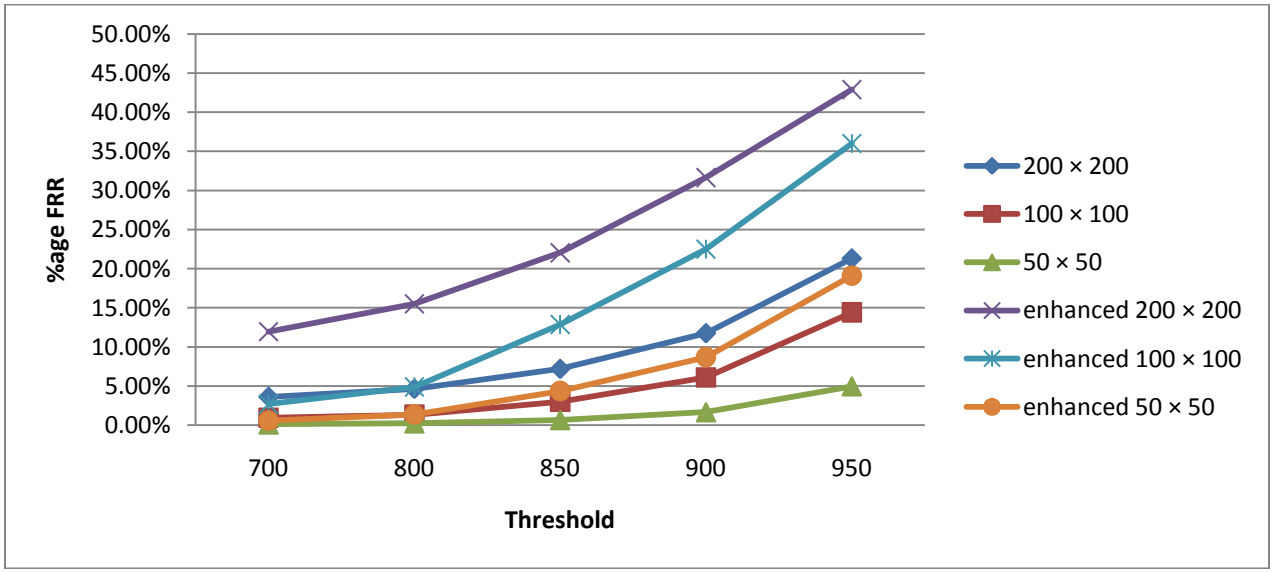


Figure 4.22 Graph between the percentage FRR and Threshold for different template size systems

On examining the Table 4.17 and Figure 4.22 it has been observed that false rejection rate (FRR) has been increasing with increase in template size i.e. FRR for 200×200 sized template image being highest and that of 50×50 sized template image being the lowest at all the threshold values. Hence, 50×50 sized template image is best while the 100×100 template

sized system is better than 200×200 sized template image system in terms of FRR. On comparing the enhanced database results with the original database results it has been observed that the later (original) are better than the former (enhanced) in all the cases at all the thresholds. For the template size of 100×100 the FRR is 2.69 % for the enhanced database in comparison to 0.94% of the original database for the same size at a threshold of 700. This is due to the fact that although with enhancement ridge-valleys structure of the fingerprint improves but much richer grey-level information of a fingerprint image had been lost.

Table 4.18 shows the false acceptance rate for different sized learning images at different thresholds for original and enhanced database and Figure 4.23 shows its graphical representation.

Table 4.18 Comparison of false acceptance rate for different learning image sizes of original and enhanced database

Threshold	**Original database (FAR)**			**Enhanced database (FAR)**		
	Template size					
	200×200	**100×100**	**50×50**	**200×200**	**100×100**	**50×50**
700	0%	0%	19.87%	0%	0%	29.45%
750	0%	0%	12.20%	0%	0%	20.025%
800	0%	0%	6.57%	0%	0%	11.65%
850	0%	0%	2.875%	0%	0%	5.675%
900	0%	0%	0.85%	0%	0%	1.725%

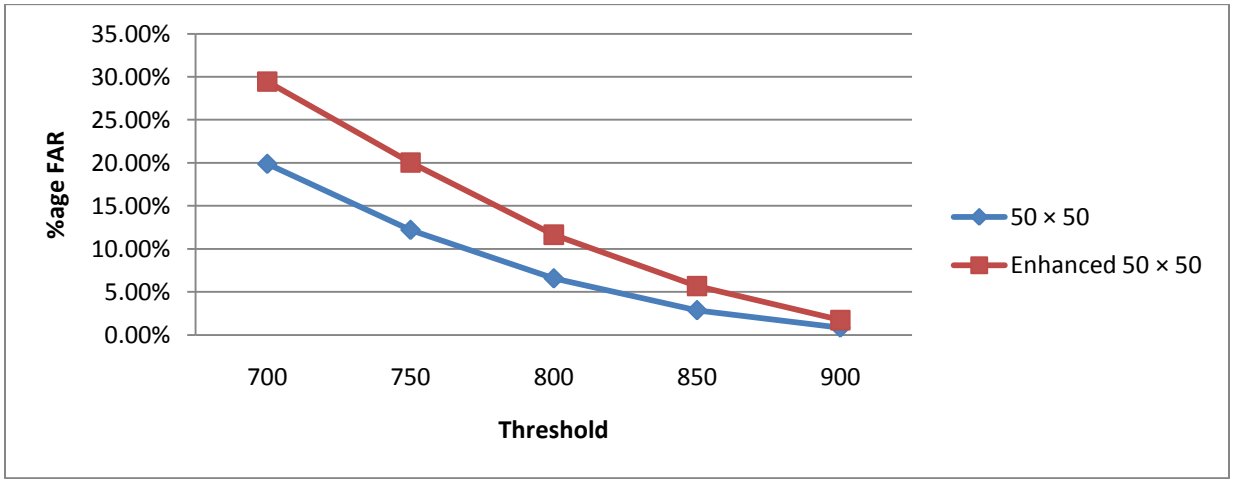


Figure 4.23 Graph between the percentage FAR and Threshold for 50×50 template size systems

False acceptance rate (FAR) is 0% for images of 200×200 and 100×100 up to the threshold of 700 as shown in Table 4.18. However, false acceptance occurs for the template size of 50×50 for both original and enhanced database. The false acceptance rate increases as threshold decreases. This is due to the fact that probability of having the same lesser information in other images (query image) is more.

Although, 50×50 template sized system results in a FRR of 0.11% in comparison to 0.94% of 100×100 template sized system and 3.61% of 200×200 template sized system at a threshold of 700, but the FAR of 19.87 % has been obtained in 50×50 in comparison to 0% in 100×100 and 200×200 sized template image at a same threshold (threshold of 700). The FAR of 50×50 sized template image decrease to 0.85% at a threshold of 900 but the false rejection rate becomes 4.97%. So, a medium sized template image of 100×100 size is the best choice among the three template sizes considered for experimentation.

4.10 Summary

In this chapter an image based fingerprint verification system has been developed and checked for the validity using the images from FVC2002/Db1_a database. A database has been created by translating, rotating and translating plus rotating the fingerprint images of FVC2002/Db1_a database. The rotation and translation between the query and reference image has been taken care by comparing the circular intensity profile of the images. The speed of the system has been increased using quasi-random sub sampling, which reduces the amount of data required for matching. The simulation results had been obtained for three different sizes of template images and for different thresholds.

The images which were translated only from the original image, no false rejection has been found for any reference template size at any threshold value. However, when images were rotated and translated plus rotated, false rejections have been found for different sized learning images. It has also been observed that as the value of the threshold go on increasing the value of false rejection rate also increases. Further, false rejection has been found to be increasing with increase in template size i.e. FRR for 200×200 sized template image being highest and that of 50×50 sized template image being the lowest at all the threshold values.

However, No false acceptance has been observed (up to threshold of 700) for the learning image size of 100×100 and 200×200 but for 50×50 size learning image considerable amount of false acceptance has been observed. These results are on the expected lines as smaller sized template images contain lesser information in comparison to larger images. Although a 50×50 sized template image system has lower FRR than 100×100 sized template image system but 100×100 sized image system has lower FAR. So, a medium sized template image of 100×100 size is the best choice among the three template sizes considered for experimentation.

Further, the fingerprint images had been enhanced using the STFT analysis and contextual filtering in the Fourier domain. The database, again, had been created by providing the required translation, rotation and translation plus rotation to the enhanced images. The simulation results had been obtained for the enhanced database. On comparing the enhanced database results with the original database results it has been observed that the later (original) are better than the former (enhanced). This is due to the fact that although with enhancement ridge-valleys structure of the fingerprint improves but much richer grey-level information of a fingerprint image had been lost. It can be concluded that the enhancement does not improve the results in case of image based systems. So, image enhancement steps should be avoided for image based fingerprint system.

In the next chapter the problems due to the single biometric system and their solutions with multimodal biometric systems will be discussed.

CHAPTER 5

Multimodal Authentication Solutions

Single biometric systems have been discussed in the chapter 3 and chapter 4. Although a single biometric system has been used in many applications such as ATM, airport security checks etc., but the single biometric system has certain drawback which must be kept in mind before its deployment for a particular application. The focus of this chapter will be to discuss the limitations of single biometric system and suggest the measures to overcome the limitations in order to enhance the system performance.

5.1 Limitations of Single Biometric System

The single biometric system suffers from the following drawbacks:

1. **Non-universality:** Universality is the basic requirement of a biometric authentication system in which every user is expected to possess the biometric trait used for verification/ identification. However, in practice the biometric trait used may not be universal i.e. every user in the population may not have the required biometric trait. For example, T. Mansfield et al. [178] reported that in fingerprint biometric system 1 in 1000 fingers are missing or have no fingerprints. P. M. Cobby et al. [179] reported a 15 % failure to enrollment problem in an iris based biometrics system. The persons who are suffering from eye abnormalities or diseases cannot provide good quality of samples for iris biometric system [180]. Similarly some people do not have hand so they cannot provide the required information for hand or palm print recognition system. In general it can be said that a single biometric trait cannot cover the entire population for a given biometric based security system.
2. **Non-uniqueness:** The characteristics of the chosen biometric system must be unique in the sense that no two individual should have the same characteristics but in practice, it may not be the case. For example, in a face recognition system due to

genetic factors identical twins or father-son may have the same facial appearance [181]. The lack of uniqueness will increase the false accept rate (FAR) of the system.

3. **Noise:** The presence of noise in the acquired biometric information may affect the accuracy of the authentication system. The noise may come into picture mainly due defective sensor or unfavorable environmental (ambient) conditions. The accumulation of dirt on the fingerprint sensor or scar on the fingerprint may add the noise component in the fingerprint based system while voice altered due to cold and blurring of the images due to non-focusing of camera are examples of noise in speaker based and face based authentication system. If the biometric system depends upon a single biometric trait than the false reject rate (FRR) will increase due to the presence of noise [182].
4. **Intra-class variation:** Biometric data obtained from the same subject may vary at different instants of time, for example, data obtained during verification/ identification may vary from the data that was obtained during enrollment. The inter class variation results due to
    (i) Improper interaction of user and the sensor
    (ii) Change in biometric traits over a period of time
    (iii) Use of different sensors during enrollment and authentication

    The inter class variation may increase the false reject rate (FRR) of the system.
5. **Circumvention:** An imposter can circumvent the system by stealing biometric traits of the authenticate user or by spoofed traits. The possibility to circumvent the system is more when behavioral traits such as voice [183] or signature [184, 185] are used than the physical traits. However, physical traits such as fingerprint can be artificially constructed to circumvent the system.

5.2 Solutions to the Problems Caused by Single Biometric

The non universality problem of single biometric system (which results in failure to enroll and/or failure to capture errors) can be taken care by using a multi-biometric system which contains more than one biometric trait. The resulting system is likely to be used by a

large population and will be perceived as user friendly since the user can choose the biometric (s) of his/her own choice.

The non uniqueness problem of single biometric can be addressed by combining biometric with the conventional authentication (knowledge/possession) systems. For example, instead of asking only the biometric trait of the person, the biometric trait and the password may be requested, which will give more security than the single biometric system or the conventional system alone. The multi biometric system can also address the problem of non-uniqueness of a single biometric trait. The introduction of more than one biometric trait can significantly improve the recognition accuracy of authentication system.

The problem of noise and intra class variation can also be addressed in a similar manner. For example, two or more than two different biometric can be fused in such a way that if one biometric trait results in a lower value of match due to noise or intra class variation and the other gives the higher value of match then the claim of the user can be accepted (some other fusion rules can also be formulated). In the biometric plus conventional system the threshold value, to accept or reject the claim of the user of biometric part may be reduced to compensate for noise and intra class variation because another security layer is also provided by the conventional system.

It becomes difficult to circumvent the combined system or multi-biometric system as it is comparatively difficult for the imposter to steal all the biometric traits of the authorized person simultaneously.

The multi-biometric system are computationally and economically more expensive than single biometric system. However, the computational time can be reduced by using a relatively simple but less accurate modality to prune the database before using the more complex and accurate modality on the remaining data to perform the final authentication.

So, in conclusion it can be said that the problems introduced by the single biometric system can be rectified by

(a) Combining a biometric modality with conventional techniques

(b) Combining more than one biometric modality i.e. multibiometric system

5.3 Combining Biometric with Conventional Techniques

Any biometric modality can be combined with the conventional methods but for the purpose of user convenience, user acceptance and low cost it has been decided to combine human voice (biometric) with the password (conventional method). The automatic recognition process of the human voice is often divided in speech recognition and speaker recognition [31,186]. These two areas use the same input signal (voice), but not for the same purpose, the speech recognition aims to recognize the message uttered by any speaker, and the speaker recognition wants to identify the person who is talking. Speaker recognition based systems are classified into two major categories speaker verification and speaker identification [5]. Speaker identification systems are used in the applications such as entry of the only authorized persons in a club or finding out a criminal from a group while speaker verification system is needed for applications like secured voice access to information (as a bank account or a voice-mail box) [31,187].

The proposed system has been developed in such a manner that firstly, it will use biometric (speaker identification) for the broader classification then narrow down its search using the password.

5.3.1 Speaker Identification

Speech and hearing, man's most used means of communication, have been the objects of intense study for more than 150 years. A speech production system is divided into following three groups [188]

(a) Lungs act as a power supply and provide airflow to the next stage larynx.

(b) Larynx modulates airflow from the lungs and provides either a periodic puff-like or a noisy airflow source to the third organ group, the vocal tract.

(c) The vocal tract consists of oral, nasal, and pharynx cavities, giving the modulated airflow its "color" by spectrally shaping the source.

Following the spectral coloring of the source by the vocal tract, the variation of air pressure at the lips results in a traveling sound wave that the listener perceives as speech. The simplified view of speech production is shown in Figure 5.1.

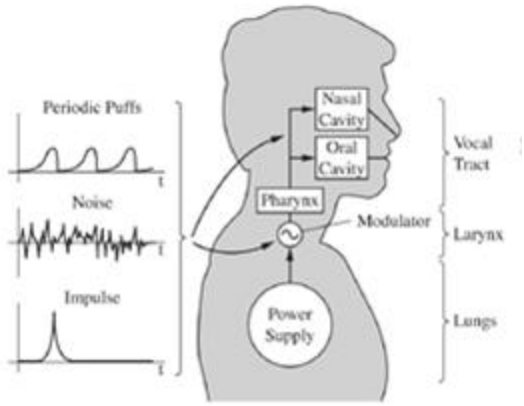


Figure 5.1 Simplified view of speech production system [188]

Voice is a combination of physiological and behavioral characteristics. The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound [188]. These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions such as common cold, emotional state and others [5]. Speaker recognition system can be text dependent or text independent. A text dependent voice recognition system is based on the utterance of a fixed predetermined phrase and a text independent voice recognition system recognizes the speaker independent of what the user speaks. However, better results are obtained by using text dependent speaker recognition, both because a control of what is said can be done and also because more accurate models (phonemes, words) can be built [189]. The process of the speaker recognition consists of the following steps:

- Speech Processing
- Feature extraction
- Pattern matching
- Decision making

The first stage of speech processing consists of recording, digitizing and preprocessing of the signal. The recording and digitizing can be performed with the help of a microphone and a sound card. The requirements of the sound card are not very stringent because of its relatively low bandwidth. The clarity of the digital sample is more dependent on the microphone quality and the environmental noise. The speech data generated by sound

card is stored in the computer. The speech waveform consists of a sequence of different events. This time variation corresponds to highly fluctuating spectral characteristics over time. It is very difficult to capture this time varying frequency content as a whole so the signal has to be divided into frames. The vocal tract is not able to change its shape faster than fifty times per second, which gives a period of 20 milliseconds [190]. So, the speech signal must be divided into frames of 20ms. This can be done with the help of a window. The most frequently used window is the hamming window [191], which is given by

$$w(n) = \begin{cases} 0.54 - 0.46\cos\left(2\pi \frac{n}{N}\right), & 0 \le n \le N \\ 0 & otherwise \end{cases} \quad (5.1)$$

The flow chart of the speech recording is shown in Figure 5.2.

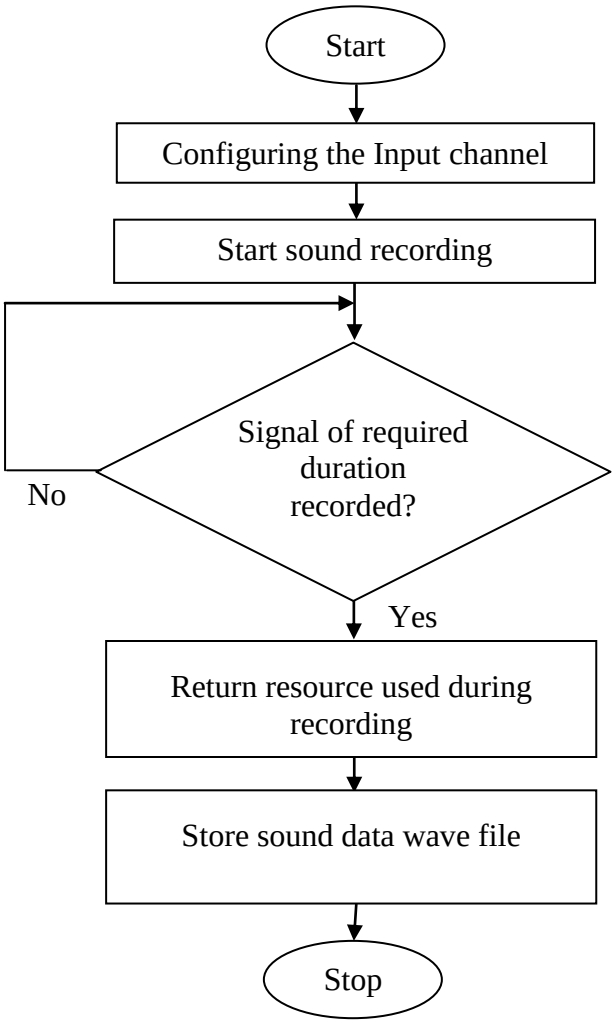


Figure 5.2 Flow chart of capturing the sound signal

Configuring the input channel means selecting the sound operation (mono or stereo), its playing rate and number of bits (8 or 16). The processing speed is another issue, which affects the performance of a speaker based recognition because a large amount of digital filtering and signal processing is involved in automatic speaker recognition. As with just about any CPU intensive software, the faster is the better. In the present case 3.0 GHz Pentium IV processor with 512 MB RAM has been used.

The choice of the feature(s) is very critical for the success of a speaker authentication system. A well chosen feature(s) can result in quality recognition while wrongly chosen feature(s) can result in a poor recognition. Many features have been described in the literature such as energy, zero cross rate, autocorrelation, linear predictive coding, mel frequency cepstral coefficient (MFCC) etc.[192]. In this work MFCC has been used since the Mel-cepstrum exploits the auditory as well as de-correlating features of the cepstrum. It is a speaker dependent feature as well. In addition Mel-cepstrum is amenable to compensation for convolution channel distortion [188]. The computation of Mel-cepstrum is shown in Figure 5.3.

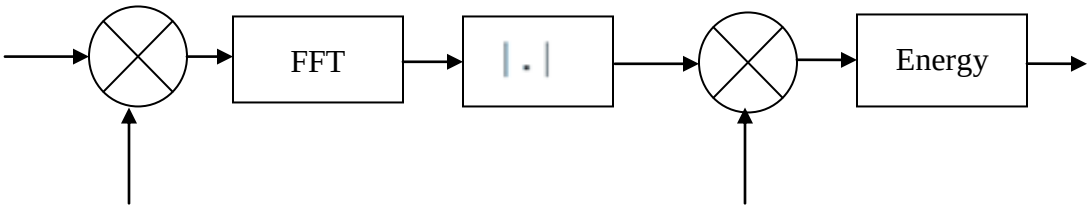


Figure 5.3 Computation of Mel-cepstrum [188]

As shown in the Figure 5.3 the STFT of the input signal has been calculated by converting the input speech signal into small pieces of 20 ms duration using Hamming window. The magnitude of STFT has been weighted with a Mel-scale filter bank and energy of resulting signal has been calculated.

If frequency response of *l*th filter is defined by $V_l(\omega)$ then resulting energies for *l*th Mel-scale filter at time n of each frame are given by:

where, L_l and U_l denote the lower and upper cutoff frequencies of the lth filter and

(5.3)

which normalizes the filters according to their varying bandwidths so as to give equal energies for flat input spectrum. The real cepstrum associated with E_{mel} is known as Mel-cepstrum and is computed as [188]:

– — (5.4)

where, m = number of cepstral coefficients and R = number of filters.

Many pattern matching algorithms for speaker identification like Minimum Distance Classifier [188, 193], Vector Quantization [194, 195], Hidden Markov Model (HMM) [196], Gaussian Mixture Model (GMM) [197] etc. have been proposed in the literature. GMM have proven to be very effective for text independent speaker recognition [198]. GMM is a density model that comprises the number of component functions. These component functions are combined to provide a multimodal density. A Gaussian mixture density is a weighted sum of k component densities [197], with

(5.5)

Where,

are the mixture weights and , x is an N by N dimensional random vector and λ is a model of speaker.

Each component density is

– (5.6)

Where, = mean vector, = N by N covariance matrix and T represents the transpose of a matrix.

The complete Gaussian mixture density is parameterized by the mean vectors, covariance matrices and mixture weights from all component densities. Each set of parameters represents the model of a speaker λ_k (,) [197-199].

The estimates of mean ( ), covariance ( ) and mixture weights ( ) is given by the Expectation maximization algorithm. For a given feature vector X(x_1,x_2,……x_m) and current estimate λ^i the EM algorithm aims to maximize with respect to unknown λ^{i+1} the expectation of the log likelihood function . This expectation over all the possible acoustic classes [200] is given by:

(5.7)

By using the above formulation that maximizing over increases the ith log likelihood i.e. . The values of unknown GMM mean covariance and weight parameters can be obtained by differentiating with respect to these unknown parameters individually and is given by [188]

– (5.8)

——————— (5.9)

——————— (5.10)

——————— (5.11)

Where is the kth pdf mixture component on the ith iteration and T in the covariance expression denotes the matrix transpose.

In the decision making stage given an utterance from an unknown speaker, the identifier simply evaluates the log likelihood – for all models and identify the person corresponding to the highest log likelihood value.

5.3.1.1 Results of Speaker Identification

To analyze the speech signal, a 256-point Hamming window has been used for calculation of STFT. The length of the frame is 20 ms and the sampling frequency used is 11025 Hz. A mel-scale band pass filter bank which is based on human auditory experiments has been created. This scale is linear up to 1 kHz and logarithmic thereafter. In the present case 40 filters have been taken, 13 of which are linearly spaced and the remaining 27 are logarithmically spaced with respect to their central frequencies. The central frequencies of

the filters have been spaced equally on the linear scale and equally on logarithmic scale above 1 kHz. Table 5.1 show the central and edge frequencies of filter bank.

Table 5.1 Central and edge frequencies of filter bank

Filter No.	Lower frequency (Hz)	Central frequency (Hz)	Upper frequency (Hz)
1	100	169.23	238.46
2	169.23	238.46	307.69
3	238.46	307.69	376.92
4	307.69	376.92	446.15
5	376.92	446.15	515.38
6	446.15	515.38	584.62
7	515.38	584.62	653.85
8	584.62	653.85	723.08
9	653.85	723.08	792.31
10	723.08	792.31	861.54
11	792.31	861.54	930.77
12	861.54	930.77	997.01
13	930.77	997.01	1067.97
14	997.01	1067.97	1143.98
15	1067.97	1143.98	1225.40
16	1143.98	1225.40	1312.61
17	1225.40	1312.61	1406.03
18	1312.61	1406.03	1506.09
19	1406.03	1506.09	1613.28
20	1506.09	1613.28	1728.10
21	1613.28	1728.10	1851.09
22	1728.10	1851.09	1928.83
23	1851.09	1928.83	2123.95
24	1928.83	2123.95	2275.11
25	2123.95	2275.11	2437.03
26	2275.11	2437.03	2610.48
27	2437.03	2610.48	2796.27
28	2610.48	2796.27	2995.28
29	2796.27	2995.28	3208.45
30	2995.28	3208.45	3436.80
31	3208.45	3436.80	3681.40
32	3436.80	3681.40	3943.40
33	3681.40	3943.40	4224.05
34	3943.40	4224.05	4524.68
35	4224.05	4524.68	4846.70
36	4524.68	4846.70	5191.65
37	4846.70	5191.65	5561.14
38	5191.65	5561.14	5956.92

39	5561.14	5956.92	6380
40	5956.92	6380	6835

The experiments have been conducted on the database of 800 samples of 80 users (10 samples for each user) out of which 50 were male and 30 were female, acquired in the laboratory in two different sessions i.e. morning and evening separated by a week. Each of the subject was requested to speak any sentence of English language for at least five second duration.

Table 5.2 Results of speaker identification

	Total number of persons	**Tests per person**	**Total tests**	**Tests passed**	**% age success**
Male	50	10	500	410	82
Female	30	10	300	250	83.3
Total	**80**	**10**	**800**	**660**	**82.5**

5.3.2 Combining Speaker Identification with Password

In the previous section speaker identification using MFCC and GMM has been explained and results obtained suggest that the best identification rate of 82.5% has been obtained. In this section study has been presented to see the effect of combining the biometric with the conventional authentication method. The system has been designed in such a way that the first stage authenticates the group of persons on the basis of biometric (speaker identification) and then in the next stage verifies the person on the basis of password. The flow chart of the proposed system has been shown in the Figure 5.4. As shown in the flow chart the MFCC features of the speech of unknown speaker has been extracted and then log likelihood of unknown speaker with each entry in the database has been calculated. To expand the possibility of matching, instead of identifying and extracting the single entry from the database, more than one entry or person (i.e. 2, 3,……) has been identified and their corresponding data has been extracted. The selection of the group has been carried out on the basis of their log likelihood values. All the log likelihood values corresponding to the unknown speaker and all the entries in the database have been arranged in the descending order and the entries with the higher log likelihood values have been selected. In the second stage the passwords (which were stored during the enrollment stage corresponding to each

entry in the database) of all the selected entries or persons in the first stage has been extracted and compared with the password entered by the unknown speaker. If the password matches with any of the entry from the selected group then the corresponding person has been identified otherwise, the system prompts the message “You are not an authorized person”.

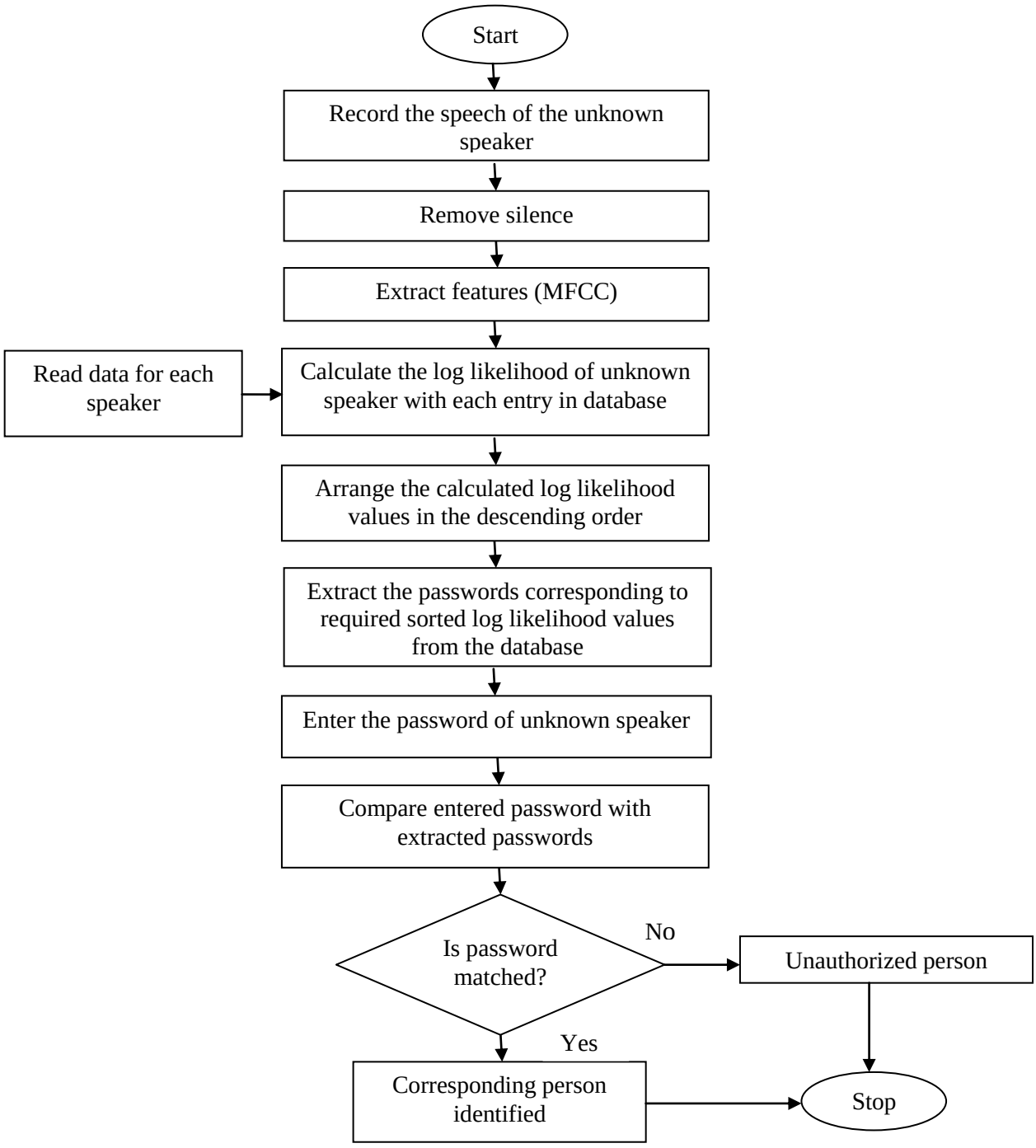


Figure 5.4 Flow chart of the proposed system

In the enrollment process of the proposed system the data record of the user is to be maintained in the database containing the name, password and λ_k (,) of the user.

5.3.2.1 Results of Proposed System

The experiments have been conducted on the same database of 800 samples of 80 persons (50 male and 30 female) on which the experiments for speaker identification had been conducted. The results in Table 5.3 have been presented on the basis of 1, 2, 3,…… up to 12 persons identified during the first stage.

Table 5.3 Results of proposed combined system

Number of entries extracted from the database during the first stage	**True identified out of 800 samples**	**Rejected samples out of 800**	**Results (in percentage)**	
			Genuine acceptance rate	**False rejection rate**
1	660	140	82.5	17.5
2	720	80	90	10
3	746	54	93.25	6.75
4	765	35	95.625	4.375
5	775	25	96.875	3.125
6	784	16	98	2
7	787	13	98.375	1.625
8	790	10	98.75	1.25
9	796	4	99.5	0.5
10	799	1	99.875	0.125
11	799	1	99.875	0.125
12	799	1	99.875	0.125

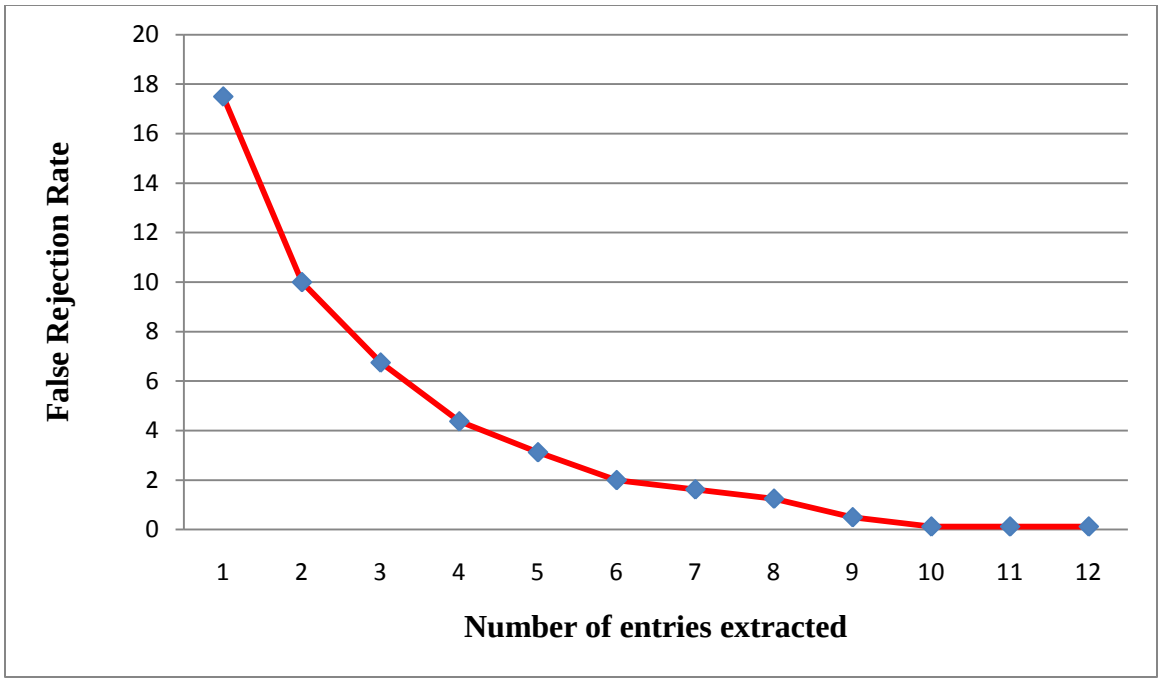


Figure 5.5 Graph between FRR and number of entries extracted in first stage

A graph between the FRR and number of entries extracted in the identification stage has been shown in the Figure 5.5. As shown in the graph the FRR goes on decreasing up to 10 entries extracted in the first stage and then becomes stable. Thus by extracting more number of entries in the identification stage, the false rejection rate error introduced in the system due to noise and intra class variation can be taken care. In the present experimentation, the database consists of 800 entries and extraction of entries from the database has little bearing on the time and performance of the system in real time. However, in practical applications with sufficiently large databases the calculation of log likelihood for all the entries can take considerable amount of time but it will not be affected by the number of entries extracted. So, number of entries to be extracted can be decided based on the success rate. In the present case 3.0 GHz Pentium IV processor with 512 MB RAM has been used which gives results in real time.

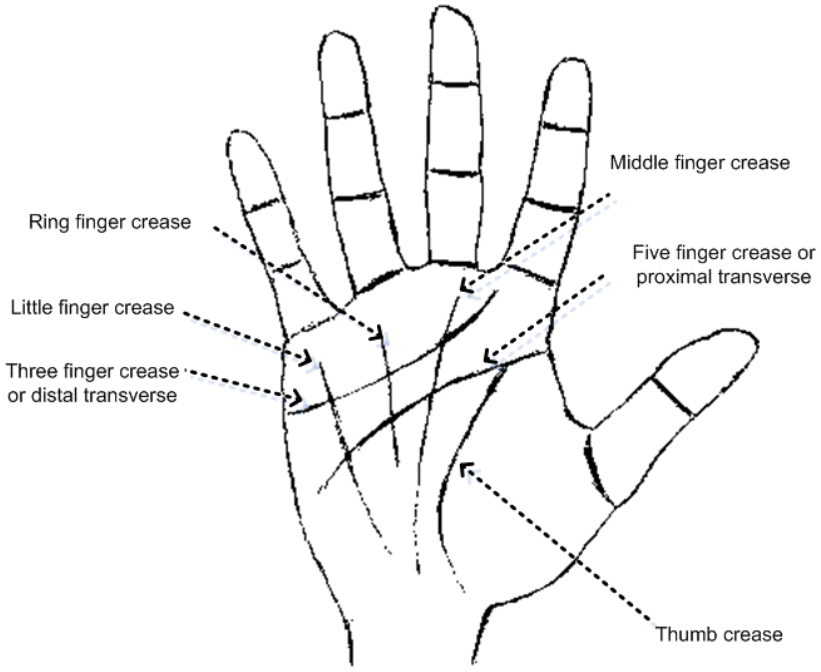
5.4 Multi-biometric System

A multi-biometric system is a biometric system that uses more than one independently or weakly correlated biometric trait taken from an individual (e.g. speech signal and fingerprints of the same person).

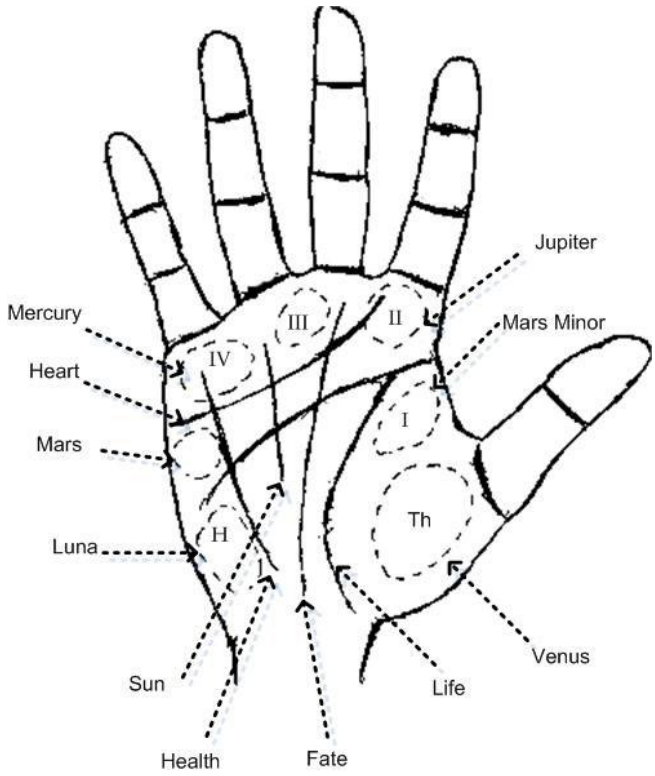
The choice and number of biometric traits used for any biometric system depends upon number of factors such as security, user acceptance, cost, user convenience, design complexity etc.. Voice or speech based biometric systems have the advantage of user convenience, user acceptance and low cost. Fingerprint based biometric systems exhibits uniqueness, consistency over time, rich feature information, acceptability and good performance. Unlike the fingerprints, palm prints cannot be acquired without the knowledge of the person or user which is very necessary in security related applications. Moreover, palm prints have medium to high performance. So, in this work it has been decided to work with these three parameters or traits of personal authentication. Since, in the previous chapters/sections, fingerprints and speech have already been discussed. So, a brief introduction of palm prints has been discussed here.

5.4.1 Palmprint

The inner surface of our palm normally contains principal lines, wrinkles and creases. There are usually three principal lines in a palmprint: the heart line, the head line, and the life line. These lines vary little over time, and their shapes and locations on the palm are the most important physiological features for individual identification. Wrinkles are much thinner than the principal lines and much more irregular. The principal lines and the main creases are formed between the 3rd and 5th months after conception [201] and petty lines appear after birth. These features are not genetic in nature. Even identical twins those are having the same DNA sequences have different palmprints [34]. These complex patterns have rich information for personal authentication. Human beings were interested in the palm lines for fortune telling long time ago. Scientists and fortunetellers name the lines and the regions differently, as shown in Figure 5.6.



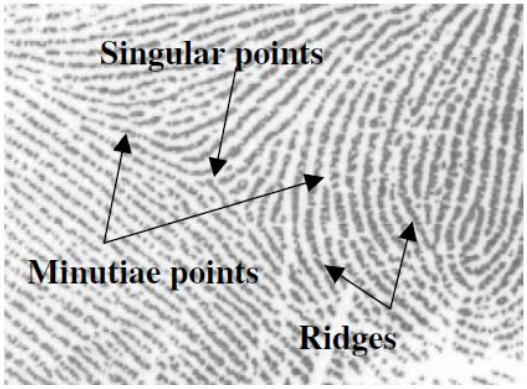
(a)



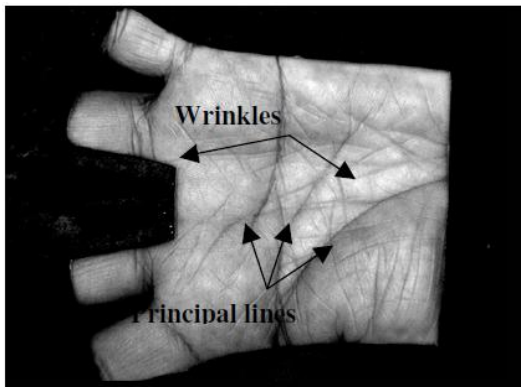
(b)

Figure 5.6 Definitions of palm lines and regions (a) from scientists and (b) from fortune-tellers

There are two types of palmprint recognition research, high resolution and low resolution approaches. High resolution approach is suitable for forensic applications such as criminal investigation, while low resolution is more suitable for civil and commercial applications such as access control. Generally speaking, high resolution refers to 400 dpi or more and low resolution refers to 150 dpi or less. Figure 5.7 illustrates a part of a high resolution palmprint image and a low resolution palmprint image. In high resolution images, researchers extract ridges, singular points and minutia points as features while in low resolution images, they generally use principal lines, wrinkles and texture.



(a)



(b)

Figure 5.7 Palmprint features in (a) High resolution image and (b) Low resolution image

Palmprint authentication system includes preprocessing, feature extraction and matching steps. The preprocessing step is used to align different palmprint images and detecting key points so that a coordinate system can be established for extracting the central parts of the palmprint. To perform the above function different approaches have been

discussed in the literature [202-206]. For feature extractions line based approach [207-209], subspace based approach [210-212], Statistical approach [213-214], Coding approach [202,215-216] etc. are used and for the purpose of palmprint matching neural networks [203], Hidden Markov Model [205], correlation filter [217] techniques etc. are present in the literature. In this work same method has been used for palmprint authentication as had been used for fingerprint authentication discussed in chapter 4.

5.4.2 Combining the Biometric Modalities

As discussed in the previous section speech, fingerprint and palmprint have been chosen as biometric modalities which are required to be combined. However, data pertaining to all of the three modalities was not available for a single set of user. Due to the mutual independence of these three modalities it has been decided to assign the standard databases of fingerprint (FVC2002_DB_1_a), palmprint (The Hongkong PolyU_Palmprint_Database 2nd Version) and recorded database of speech to subject 1, subject 2, ……., subject 40. For the purpose of experimentation, the database of fingerprint and palmprint was rotated, translated and translated plus rotated by $\pm 1^{o}$ and ± 1 pixel in x and y direction up to $\pm 15^{o}$ and ± 15 pixels respectively. In this way for each image of fingerprint and palmprint has 90 rotated, translated and translated plus rotated images.

Thus a database having $90 \times 40 = 3600$ fingerprint images, $90 \times 40 = 3600$ palmprint images and $80 \times 10 = 800$ speech signals, has been created.

It has been decided to combine fingerprint and palmprint biometric traits. Some fusion techniques like sum rule, decision tree rule, weighted tree rule are present in the literature but in the present work it has been decided to use fuzzy logic to combine (fuse) fingerprint and palm print at score level.

5.4.3 Fuzzy Logic

Fuzzy logic is a way of processing data by accepting noise and imprecise input. It provides a simply way to arrive at a definite conclusion based on vague, ambiguous, imprecise, noisy or missing input information. Fuzzy logic approach mimics, the way in which a human make decisions, but it is much faster than human brain. Fuzzy logic can be

termed as problem – solving methodology that can be implemented in systems ranging from simple, small, embedded microcontrollers to large, networked, multi-channel PC or workstation-based systems. It can be implemented in hardware, software, or a combination of both [218]. Fuzzy logic is an approach to computing based on "degrees of truth" rather than the usual "true or false" (1 or 0) Boolean logic on which the modern computer is based. Fuzzy logic not only includes 0 and 1 as extreme cases of truth (or "the state of matters" or "fact") but also includes the various states of truth in between these two values.

Fuzzy Logic offers several unique features that make it a particularly good choice for authentication problem. Some of these are

1. Fuzzy logic is conceptually easy to understand. The mathematical concepts behind fuzzy reasoning are very simple and are easy to understand. This property makes it one of the favorable techniques [219].
2. Fuzzy logic technique is based upon the simple rules, which are easy to apply and can be modified easily to improve the system performance [220].
3. Because of the rule-based operation, any reasonable number of inputs can be processed and reasonable number of outputs can be generated, although defining the rule base quickly becomes complex if too many inputs and outputs are chosen for a single implementation [221] .
4. Fuzzy Logic can control nonlinear systems that would be difficult or impossible to model mathematically [221].

5.4.4 Steps for Fuzzy Logic Implementation

Following steps have been used for the implementation of fuzzy logic [222]:

(i) **Define the Universe of Discourse**

The first step for the designing of a fuzzy logic controller requires to define all the input and output variables along with the range of values that the inputs and outputs may take. In the present case score of fingerprint and palmprint are the inputs while the claim of authentication of the person is the output. Table 5.4 shows the universe of discourse for the inputs and output.

Table 5.4 Universe of discourse for the inputs and output

Name	Input/ Output	Minimum Value	Maximum Value
Fingerprint	Input	0	1000
Palmprint	Input	0	1000
Claim of authentication	Output	0	1000

(ii) **Setup Fuzzy Membership Functions for Inputs**

Fuzzification is a process where the crisp quantities are converted to fuzzy quantities [223]. In the present case, fingerprint and palmprint are inputs with the crisp values ranging from 0 to 1000. Experiments have been conducted to find out the optimum number of fuzzy variable and ultimately, low, medium, high and very high fuzzy variables have been chosen. Table 5.5 shows the assignment of ranges and membership functions to different variables of fuzzy set both for fingerprint and palmprint.

Table 5.5 Fuzzy variable ranges and membership functions for fingerprint and palmprint

Crisp input range	Fuzzy variable	Membership function
0 – 700	Low	Trapezoidal
600 – 800	Medium	Triangular
700 – 900	High	Triangular
800 – 1000	very high	Trapezoidal

Figure 5.8 and Figure 5.9 represents the fuzzy membership function for fingerprint and palmprint respectively.

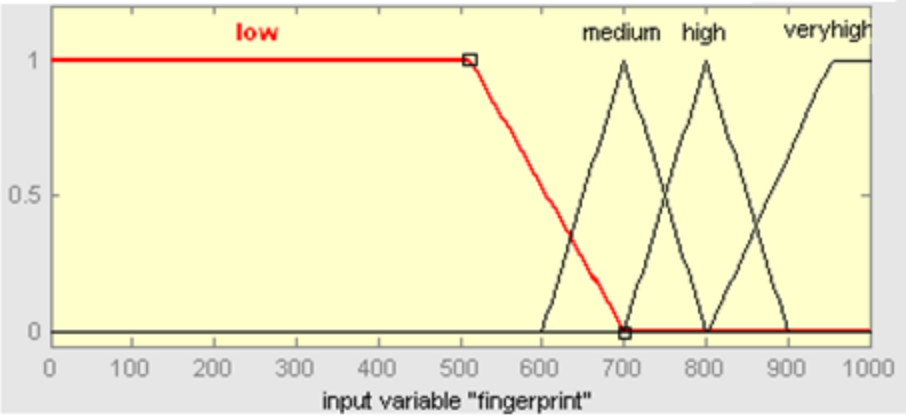


Figure 5.8 Fuzzy membership function for fingerprint

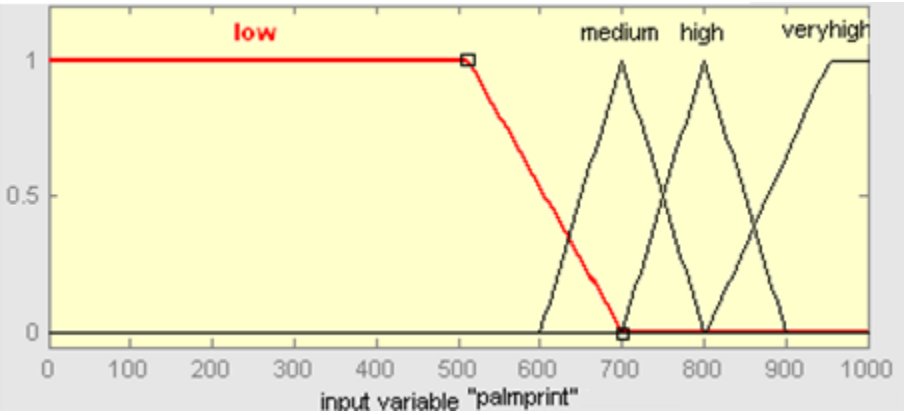


Figure 5.9 Fuzzy membership function for palmprint

(iii) **Setup Fuzzy Membership Functions for the Output(s)**

The next step in the design of fuzzy logic is to set up fuzzy membership functions for the outputs. The present case has only one output, that is, the claim of the user for authenticity. Fuzzy memberships to this variable have been defined in the similar manner as has been defined for the inputs. Table 5.6 and Figure 5.10 shows the range, fuzzy variables and the membership functions used for the output variable.

Table 5.6 Fuzzy variable ranges and membership functions for output variable

Crisp range	**Fuzzy variable**	**Membership function**
0 – 500	Reject	Trapezoidal
300 – 700	Reenter	Triangular
500 – 1000	Accept	Trapezoidal

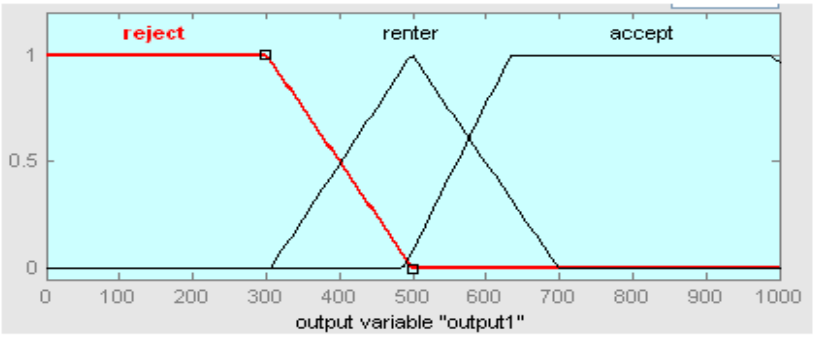


Figure 5.10 Fuzzy membership function for the output variable

(iv) **Create a Fuzzy Rule Base**

Rules form the basis for the fuzzy logic to obtain the fuzzy output. Fuzzy rules are a collection of linguistic statements in the form of IF-THEN rules that may mimic the behavior of a human being while making a decision. Fuzzy rules are written in the following form:

If (fingerprint is very high) **AND/OR** (palm print is very high) **then** (output is accept)

In the above statement, if-part of the rule "fingerprint is very high/ palm print is very high" is called the antecedent, while the then-part of the rule "output is accept" is called the consequent. If in a rule there are more than one antecedent (as in the case of above rule) then logical operators are required to obtain one value that represents the result of antecedent for that rule. **AND/OR** in the above statement are known as logical operators.

The number and complexity of rules depends on the number of input parameters that are to be processed and the number fuzzy variables associated with each parameter. In the present case different fuzzy input variables of fingerprint, palmprint and fuzzy output variables are combined to formulate the IF-THEN rules for biometric security systems. All these rules are described in the next section and to evaluate more than one antecedents AND logical operator with min function has been used.

(v) **Apply Implication Method**

The next step is to correlating the rules of consequent with the truth value of the antecedent value to obtain the output fuzzy set. This can be done with the help of implication method. The input for the implication process is a single number given by the antecedent and the output is a fuzzy set. The most common methods of implication are clipping (min) and scaling (prod). In the method of clipping consequent membership function is cut at the level of the antecedent truth while in scaling the original membership function of the rule consequent is adjusted by multiplying all its membership degrees by the truth value of the rule antecedent. Clipping is often preferred method of implication because it involves less complex and faster mathematics and generates an aggregated output surface that is easier to defuzzify. In the present work, clipping (min) has been used as an implication method.

(vi) **Aggregate All Outputs**

Aggregation is the process by which the fuzzy sets that represent the outputs of each rule are combined into a single fuzzy set. The input of the aggregation process is the list of truncated output functions returned by the implication process for each rule. The output of the aggregation process is one fuzzy set for each output variable. Three aggression methods max (maximum), probor (probabilistic OR), and sum (simply the sum of each rule's output set) are commonly used. In the present work max aggression method has been used.

(vii) **Defuzzify the output (s)**

The last step in the fuzzy inference process is defuzzification. Fuzziness helps us to evaluate the rules, but the final output of a fuzzy system has to be a crisp number. Defuzzification means fuzzy to crisp conversion [223, 224]. The input for the defuzzification process is the aggregate output fuzzy set and the output is a single number. Many defuzzification methods like maximum membership, weighted average, centroid, centre of sums, centre of largest area etc., are available in literature. Among all these methods centroid method is most commonly used and is also known as centre of gravity method. In the present work centroid method for defuzzification has been used.

5.4.5 Different Security Systems

The system that uses biometric for security applications can be classified into three different categories depending upon the importance of a particular application. These are:

i) Low security system
ii) Medium security system
iii) High security system

Low security systems can be used in such situations where breach of security does not have a long lasting impact (in terms of financial concerns and loss to human being) on the society such as attendance of the students/ employees in a university/ company or issue/ return of book(s) from a library etc.. The low security system aims to have a very low false rejection rate. High security systems are employed in very critical situations such as defense related applications, protection of foreign policy documents, security for intelligence information etc.. In applications, where high security is required, the false acceptance should be as low as possible, while false rejection can occur to some extent in the system. Medium security system includes applications such as physical access control, logical access control, operation of ATM, operation of mobiles and laptops etc.. Medium security system is a tradeoff between high security and low security. In other words, medium security system aims

to have low false acceptance rate than low security and low false rejection rate in comparison to high security system.

Realizing the requirements of different security systems, various rules have been framed for different security systems i.e. low, medium and high. While low security system has to be oriented towards low FRR, the high security system looks for zero false acceptance rate. The results of all the three i.e. low, medium and high security systems have been analyzed in detail in the following section.

5.4.5.1 Rules for Low Security

The rules for a low security system have been formulated in such a way that if any of the inputs is very high or high then the system must give a high output i.e. the system should accept the claim of the user. On the other hand if the input from the fingerprint is low and from palmprint is low or medium then the claim of the user must be rejected. For all other cases the user should be asked to enter the biometric traits again. The various rules that have been defined for the different combination of inputs (fingerprint and palmprint) and output, in a low security system are given below:

1. If (fingerprint is very high) AND (palmprint is very high) then (output is Accept)
2. If (fingerprint is very high) AND (palmprint is high) then (output is Accept)
3. If (fingerprint is very high) AND (palmprint is medium) then (output is Accept)
4. If (fingerprint is very high) AND (palmprint is low) then (output is Accept)
5. If (fingerprint is high) AND (palmprint is very high) then (output is Accept)
6. If (fingerprint is high) AND (palmprint is high) then (output is Accept)
7. If (fingerprint is high) AND (palmprint is medium) then (output is Accept)
8. If (fingerprint is high) AND (palmprint is low) then (output is Accept)
9. If (fingerprint is medium) AND (palmprint is very high) then (output is Accept)
10. If (fingerprint is medium) AND (palmprint is high) then (output is Accept)
11. If (fingerprint is medium) AND (palmprint is medium) then (output is renter)
12. If (fingerprint is medium) AND (palmprint is low) then (output is renter)
13. If (fingerprint is low) AND (palmprint is very high) then (output is Accept)

14. If (fingerprint is low) AND (palmprint is high) then (output is Accept)
15. If (fingerprint is low) AND (palmprint is medium) then (output is reject)
16. If (fingerprint is low) AND (palmprint is low) then (output is reject)

5.4.5.2 Rules for Medium Security

For a medium security system the if- then rules have been formulated in a manner that the claim of the user is accepted only if both the inputs individually are very high or high at the same time. On the other hand the claim of the user is rejected if any of the inputs is low and if both the inputs have medium value. For all other cases the user should be asked to enter the biometric traits again. The various rules that have been defined for the different combination of inputs (fingerprint and palmprint) and output, in a medium security system are given below:

1. If (fingerprint is very high) AND (palmprint is very high) then (output is Accept)
2. If (fingerprint is very high) AND (palmprint is high) then (output is Accept)
3. If (fingerprint is very high) AND (palmprint is medium) then (output is renter)
4. If (fingerprint is very high) AND (palmprint is low) then (output is reject)
5. If (fingerprint is high) AND (palmprint is very high) then (output is Accept)
6. If (fingerprint is high) AND (palmprint is high) then (output is Accept)
7. If (fingerprint is high) AND (palmprint is medium) then (output is renter)
8. If (fingerprint is high) AND (palmprint is low) then (output is reject)
9. If (fingerprint is medium) AND (palmprint is very high) then (output is renter)
10. If (fingerprint is medium) AND (palmprint is high) then (output is renter)
11. If (fingerprint is medium) AND (palmprint is medium) then (output is reject)
12. If (fingerprint is medium) AND (palmprint is low) then (output is reject)
13. If (fingerprint is low) AND (palmprint is very high) then (output is reject)
14. If (fingerprint is low) AND (palmprint is high) then (output is reject)
15. If (fingerprint is low) AND (palmprint is medium) then (output is reject)
16. If (fingerprint is low) AND (palmprint is low) then (output is reject)

5.4.5.3 Rules for High Security

For a high security system the if- then rules have been formulated in a manner that the claim of the user is accepted only if both the inputs individually are very high or high at the same time. On the other hand the user is asked to enter the biometric traits again if one of the inputs is very high and other is medium. For all other cases the claim of the user is rejected. The various rules that have been defined for the different combination of inputs (fingerprint and palmprint) and output, in a high security system are given below:

1. If (fingerprint is very high) AND (palmprint is very high) then (output is Accept)
2. If (fingerprint is very high) AND (palmprint is high) then (output is Accept)
3. If (fingerprint is very high) AND (palmprint is medium) then (output is renter)
4. If (fingerprint is very high) AND (palmprint is low) then (output is reject)
5. If (fingerprint is high) AND (palmprint is very high) then (output is Accept)
6. If (fingerprint is high) AND (palmprint is high) then (output is Accept)
7. If (fingerprint is high) AND (palmprint is medium) then (output is reject)
8. If (fingerprint is high) AND (palmprint is low) then (output is reject)
9. If (fingerprint is medium) AND (palmprint is very high) then output is reenter
10. If (fingerprint is medium) AND (palmprint is high) then (output is reject)
11. If (fingerprint is medium) AND (palmprint is medium) then output reject
12. If (fingerprint is medium) AND (palmprint is low) then output reject
13. If (fingerprint is low) AND (palmprint is very high) then (output is reject)
14. If (fingerprint is low) AND (palmprint is high) then (output is reject)
15. If (fingerprint is low) AND (palmprint is medium) then (output is reject)
16. If (fingerprint is low) AND (palmprint is low) then (output is reject)

Figure 5.11 shows the flow chart of the fuzzy logic based security system. As shown in the flow chart first of all the person asserts its identity and provides the biometric information i.e. fingerprint and palmprint. Both these biometrics are processed to extract the features. The features of fingerprint and palmprint of the corresponding person are extracted from the database. A comparison has been made between the features of the query images with the corresponding features of the reference set. A similarity score has been calculated

for both the biometrics and fed to the fuzzy inference system for verification. Depending upon the formulated if-else rule and defuzzification method used the fuzzy inference generates a crisp value. If this value is greater than a predefined threshold value then the claim of the user should be accepted and access should be provided to the user. If the crisp value is less than the lower threshold then claim of the user should be rejected. On the other hand, if the value is between upper and lower threshold then the person has been asked to provide the second stage biometric features again and this process will terminate after three such attempt. However, depending upon the importance of the application the number of attempts for reenter may be increased or decreased e.g. for high security system reenter option may be decreased to zero.

Table 5.7 shows the results of genuine acceptance rate of low, medium and high security systems using the fuzzy logic while Table 5.8 shows the false rejection rate (FRR) of low, medium and high security systems using the fuzzy logic.

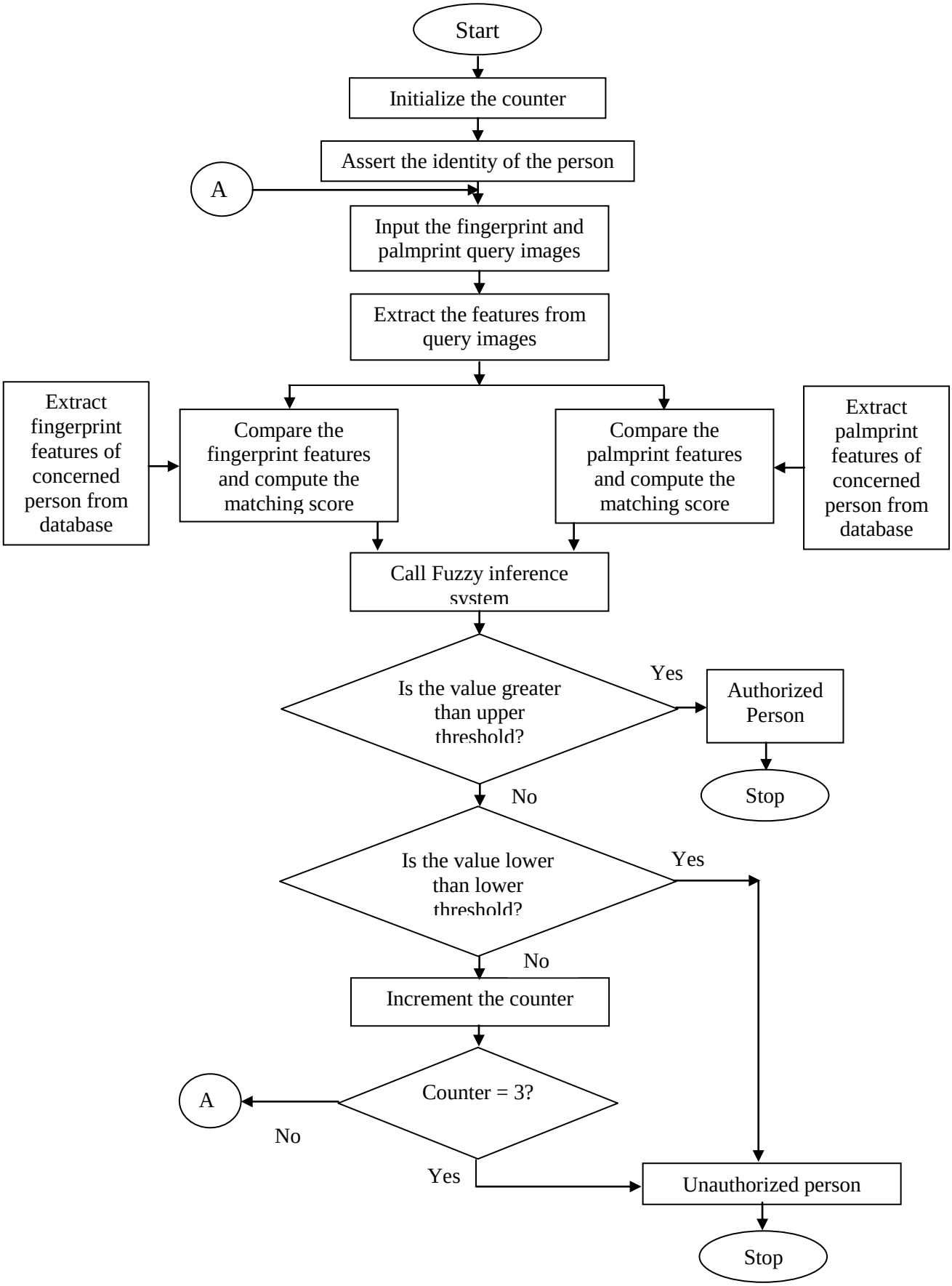


Figure 5.11 Flow chart for the fuzzy logic based different security systems

Table 5.7 Genuine acceptance rate of low, medium and high security systems using the fuzzy logic

Biometric Sample	Accept			Renter			Reject		
	Low	Medium	High	Low	Medium	High	Low	Medium	High
Subject 1	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 2	100.00%	96.67%	96.67%	0.00%	3.33%	3.33%	0.00%	0.00%	0.00%
Subject 3	100.00%	96.67%	96.67%	0.00%	3.33%	0.00%	0.00%	0.00%	3.33%
Subject 4	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 5	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 6	100.00%	96.67%	96.67%	0.00%	3.33%	0.00%	0.00%	0.00%	3.33%
Subject 7	100.00%	93.33%	90.00%	0.00%	6.67%	6.67%	0.00%	0.00%	3.33%
Subject 8	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 9	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 10	100.00%	86.67%	86.67%	0.00%	6.67%	0.00%	0.00%	6.67%	13.33%
Subject 11	100.00%	100.00%	96.67%	0.00%	0.00%	3.33%	0.00%	0.00%	0.00%
Subject 12	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 13	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 14	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 15	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 16	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 17	100.00%	93.33%	93.33%	0.00%	6.67%	6.67%	0.00%	0.00%	0.00%
Subject 18	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 19	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 20	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 21	100.00%	100.00%	93.33%	0.00%	0.00%	6.67%	0.00%	0.00%	0.00%
Subject 22	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 23	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 24	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 25	100.00%	90.00%	90.00%	0.00%	10.00%	0.00%	0.00%	0.00%	10.00%
Subject 26	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 27	100.00%	96.67%	93.33%	0.00%	3.33%	6.67%	0.00%	0.00%	0.00%
Subject 28	100.00%	100.00%	93.33%	0.00%	0.00%	3.33%	0.00%	0.00%	3.33%
Subject 29	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 30	100.00%	96.67%	90.00%	0.00%	3.33%	3.33%	0.00%	0.00%	6.67%
Subject 31	100.00%	93.33%	90.00%	0.00%	6.67%	6.67%	0.00%	0.00%	3.33%
Subject 32	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 33	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 34	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 35	100.00%	100.00%	93.33%	0.00%	0.00%	6.67%	0.00%	0.00%	0.00%
Subject 36	100.00%	83.33%	76.67%	0.00%	16.67%	6.67%	0.00%	0.00%	16.67%
Subject 37	100.00%	100.00%	96.67%	0.00%	0.00%	3.33%	0.00%	0.00%	0.00%
Subject 38	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 39	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Subject 40	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

Table 5.8 False rejection rate of low, medium and high security systems using the fuzzy logic

Biometric Sample	Low	Medium	High
Subject 1	0.00%	0.00%	0.00%
Subject 2	0.00%	3.33%	3.33%
Subject 3	0.00%	3.33%	3.33%
Subject 4	0.00%	0.00%	0.00%
Subject 5	0.00%	0.00%	0.00%
Subject 6	0.00%	3.33%	3.33%
Subject 7	0.00%	6.67%	10.00%
Subject 8	0.00%	0.00%	0.00%
Subject 9	0.00%	0.00%	0.00%
Subject 10	0.00%	13.33%	13.33%
Subject 11	0.00%	0.00%	3.33%
Subject 12	0.00%	0.00%	0.00%
Subject 13	0.00%	0.00%	0.00%
Subject 14	0.00%	0.00%	0.00%
Subject 15	0.00%	0.00%	0.00%
Subject 16	0.00%	0.00%	0.00%
Subject 17	0.00%	6.67%	6.67%
Subject 18	0.00%	0.00%	0.00%
Subject 19	0.00%	0.00%	0.00%
Subject 20	0.00%	0.00%	0.00%
Subject 21	0.00%	0.00%	6.67%
Subject 22	0.00%	0.00%	0.00%
Subject 23	0.00%	0.00%	0.00%
Subject 24	0.00%	0.00%	0.00%
Subject 25	0.00%	10.00%	10.00%
Subject 26	0.00%	0.00%	0.00%
Subject 27	0.00%	3.33%	6.67%
Subject 28	0.00%	0.00%	6.67%
Subject 29	0.00%	0.00%	0.00%
Subject 30	0.00%	3.33%	10.00%
Subject 31	0.00%	6.67%	10.00%
Subject 32	0.00%	0.00%	0.00%
Subject 33	0.00%	0.00%	0.00%
Subject 34	0.00%	0.00%	0.00%
Subject 35	0.00%	0.00%	6.67%
Subject 36	0.00%	16.67%	23.33%
Subject 37	0.00%	0.00%	3.33%
Subject 38	0.00%	0.00%	0.00%
Subject 39	0.00%	0.00%	0.00%
Subject 40	0.00%	0.00%	0.00%

In all there are total 40 different images and 90 versions of each image so total images are 3600. Table 5.9 shows the consolidated false rejection rate results for low security, medium security and high security system.

Table 5.9 Consolidated results of false rejection rate for different security systems

	Low security system	**Medium security system**	**High security system**
Total true images rejected by the system (out of 3600)	0	58	104
False Rejection Rate	**0%**	**1.61%**	**2.88%**

False acceptance rate is the measure of wrongly accepting the claim of the imposter (unauthorized person). To find out the false acceptance rate of a system it is required to match the features of the reference image of one person stored in the data base to the features of the query image of some other person to find out if any correspondence exists between the two images. For example, the features of subject 1 are compared with the features of the subject 2, subject 3 and so on. The simulations results obtained are presented in Table 5.10. Each set of images in one subject has been compared with 100 set of images for other subjects.

Table 5.10 False acceptance rate of low, medium and high security systems using the fuzzy logic

Biometric Sample	**Low**	**Medium**	**High**
Subject 1	0.00%	0.00%	0.00%
Subject 2	0.00%	0.00%	0.00%
Subject 3	4.00%	0.00%	0.00%
Subject 4	0.00%	0.00%	0.00%
Subject 5	6.00%	0.00%	0.00%
Subject 6	0.00%	0.00%	0.00%
Subject 7	4.00%	0.00%	0.00%
Subject 8	0.00%	0.00%	0.00%
Subject 9	0.00%	0.00%	0.00%
Subject 10	0.00%	0.00%	0.00%
Subject 11	0.00%	0.00%	0.00%

Subject 12	4.00%	1.00%	0.00%
Subject 13	0.00%	0.00%	0.00%
Subject 14	0.00%	0.00%	0.00%
Subject 15	0.00%	0.00%	0.00%
Subject 16	0.00%	0.00%	0.00%
Subject 17	2.00%	1.00%	0.00%
Subject 18	0.00%	0.00%	0.00%
Subject 19	2.00%	2.00%	0.00%
Subject 20	0.00%	0.00%	0.00%
Subject 21	0.00%	0.00%	0.00%
Subject 22	0.00%	0.00%	0.00%
Subject 23	2.00%	2.00%	0.00%
Subject 24	0.00%	0.00%	0.00%
Subject 25	0.00%	0.00%	0.00%
Subject 26	0.00%	0.00%	0.00%
Subject 27	0.00%	0.00%	0.00%
Subject 28	0.00%	0.00%	0.00%
Subject 29	0.00%	0.00%	0.00%
Subject 30	3.00%	2.00%	0.00%
Subject 31	1.00%	0.00%	0.00%
Subject 32	0.00%	0.00%	0.00%
Subject 33	0.00%	0.00%	0.00%
Subject 34	0.00%	0.00%	0.00%
Subject 35	2.00%	0.00%	0.00%
Subject 36	0.00%	0.00%	0.00%
Subject 37	0.00%	0.00%	0.00%
Subject 38	0.00%	0.00%	0.00%
Subject 39	0.00%	0.00%	0.00%
Subject 40	0.00%	0.00%	0.00%

Table 5.11 shows the consolidated false acceptance rate results for low security, medium security and high security system.

Table 5.11 Consolidated results of false acceptance rate for different security systems

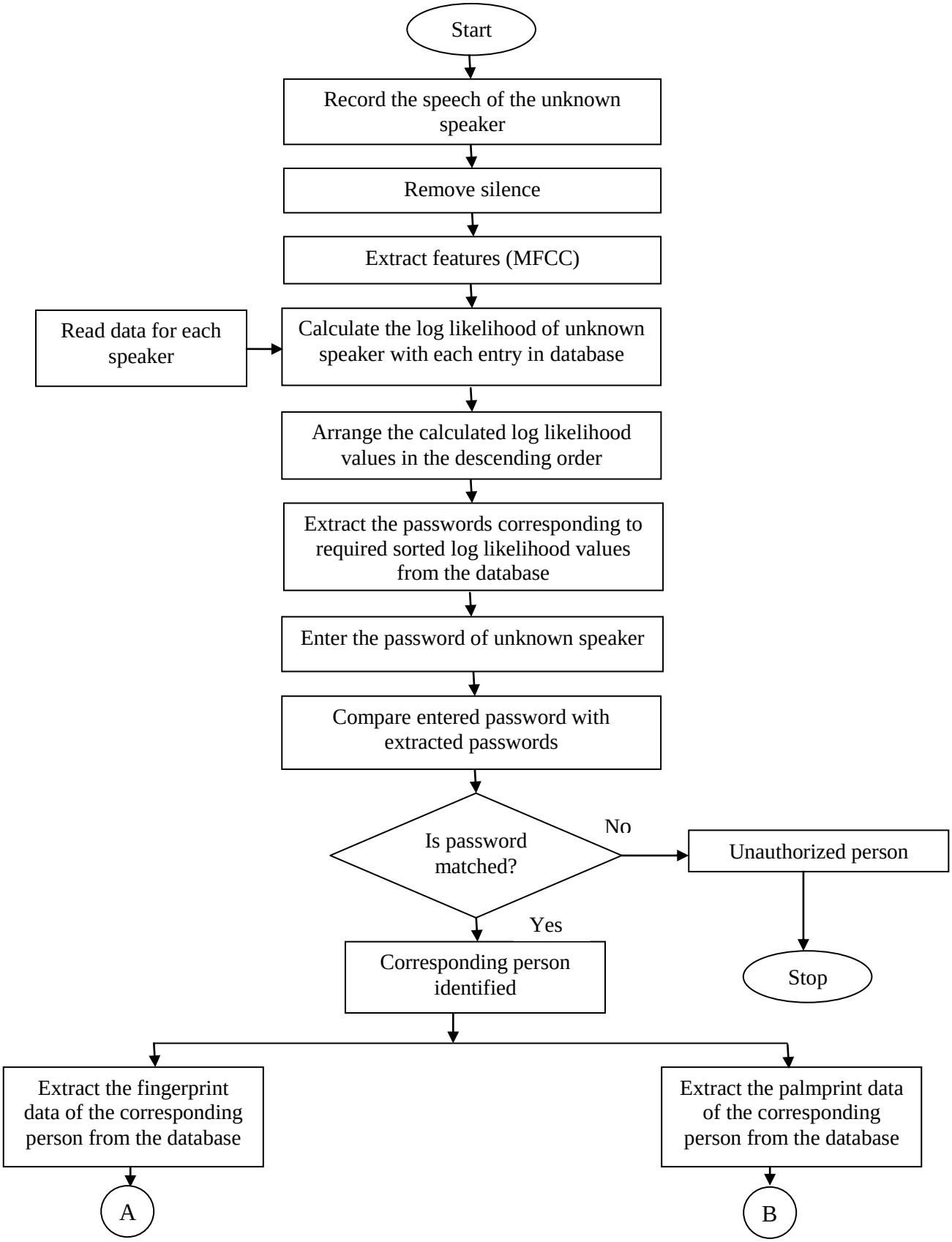
	Low security system	**Medium security system**	**High security system**
Total true images accepted by the system (out of 4000)	30	9	0
False Acceptance Rate	**0.75%**	**0.225%**	**0%**

Table 5.9 and 5.11 indicates the false rejection rate and false acceptance rate for low medium and high security systems. As is clear from the results that false rejection rate of low security system is less and false acceptance rate is high, while for high security system false rejection rate is high and false acceptance rate is very low. The low security systems may be utilized to overcome the problem of non universality and high security systems for the non uniqueness.

5.5 Very High Security Systems

Proposed medium and high security systems have provided a reasonable performance measure i.e. false rejection rate and false acceptance rate but still in an application where it is required to provide a very high security such as access to the nuclear weapons, false acceptance cannot be tolerated at all (should be zero), although, reasonable false rejection can be tolerated in the system. For a very high security system another layer of security, i.e. Speaker identification with password, may be added to the high security system. The flow chart of the very high security system is shown in Figure 5.12. The system has been designed in such a manner that in the first stage the person is identified based upon the speech biometric and the password. The second stage authenticates the user based upon the level of matching between the reference features and the features provided by the biometric traits i.e. fingerprint and palmprint.

If the person is not enrolled (not in the database) or is an unauthorized person or provides wrong information then the system stops at the first stage and do not process further to give access to the imposter. On the other hand if the person is identified then the system will go to the second stage for authentication using fingerprint and palmprint through fuzzy logic system. Such a system will overcome the problem of non uniqueness and intra-class variation effectively.


Start
Record the speech of the unknown speaker
Remove silence
Extract features (MFCC)
Read data for each speaker
Calculate the log likelihood of unknown speaker with each entry in database
Arrange the calculated log likelihood values in the descending order
Extract the passwords corresponding to required sorted log likelihood values from the database
Enter the password of unknown speaker
Compare entered password with extracted passwords
Is password matched?
No
Unauthorized person
Stop
Yes
Corresponding person identified
Extract the fingerprint data of the corresponding person from the database
Extract the palmprint data of the corresponding person from the database
A
B

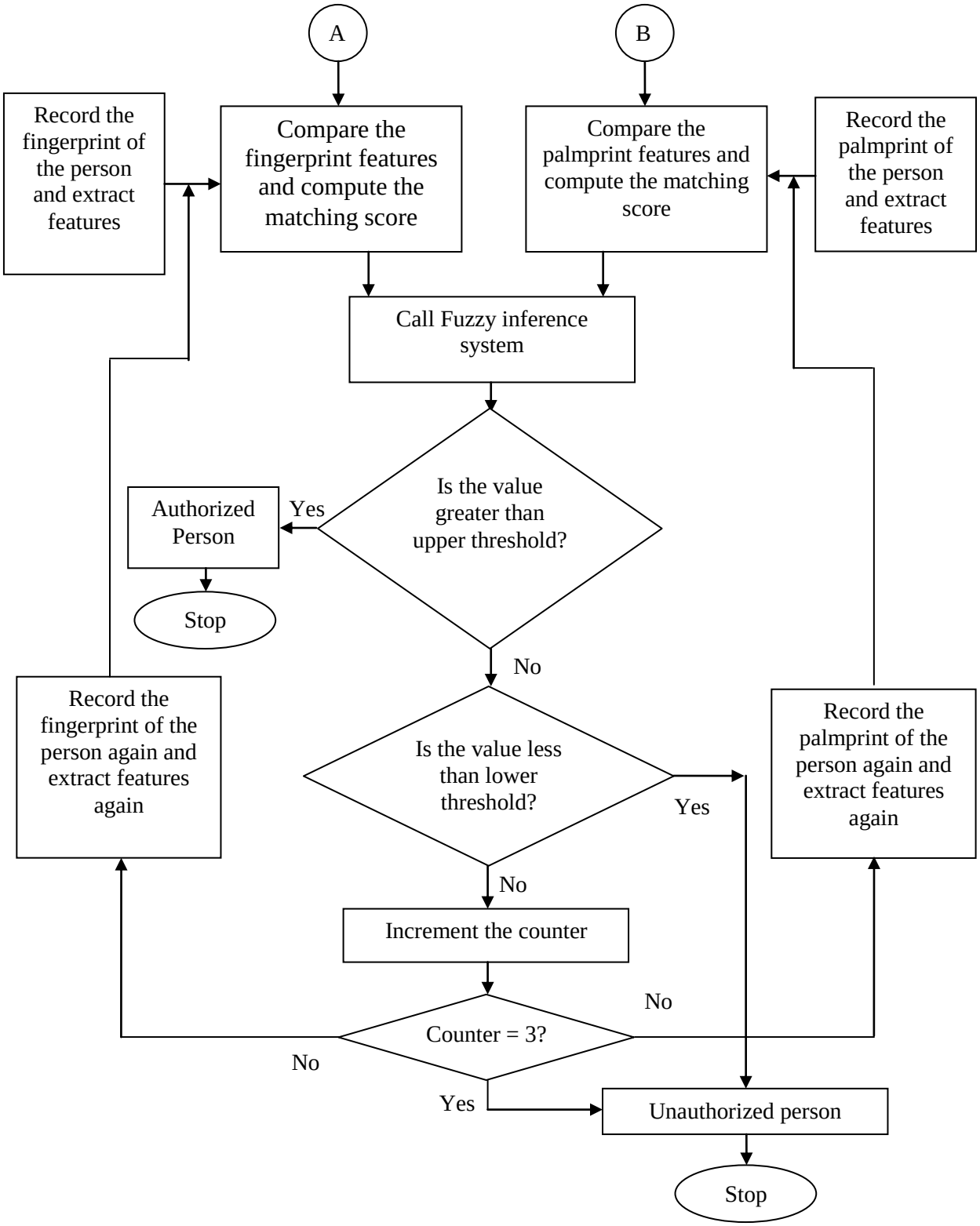


Figure 5.12 Flow chart of very high security system

5.5.1 Results of Very High Security System

In a very high security system two systems speaker identification and fuzzy logic system using fingerprint and palmprint have connected in cascade. Since the data pertaining to all the three modalities was not available for a single set of users. So the data of 80 users of speech (with 10 samples of each) was randomly paired with images from fingerprint and palmprint databases (with 10 samples of rotated, translated and rotated plus translated versions of same image randomly chosen) for the purpose of experimentation. The simulated results thus obtained for very high security system are given in Table 5.12.

Table 5.12 Results of very high security system

Number of entries extracted from the database during the first stage	**True identified out of 800 Samples**	**Rejected samples out of 800**	**Results (in percentage)**	
			Genuine Acceptance rate	**False Rejection Rate**
1	646	154	80.75	19.25
2	734	66	91.75	8.25
3	729	71	91.125	8.875
4	739	61	92.375	7.625
5	753	47	94.125	5.875
6	762	38	95.25	4.75
7	764	36	95.5	4.5
8	766	34	95.75	4.25
9	772	28	96.5	3.5
10	775	25	96.875	3.125
11	775	25	96.875	3.125
12	775	25	96.875	3.125

Although, the addition of another stage in a system provides better security but this stage has increased the false rejection rate and will also add up to the user discomfort.

5.6 Summary

In this chapter various limitations of single biometric system have been discussed. Two solutions have been proposed and implemented to overcome these limitations. In the first solution, a system combining single biometric (speech) and conventional method (password) has been developed. The system has been designed in such a manner that the first stage identifies the group of persons on the basis of biometric (speaker identification) and second stage verifies the person on the basis of password from the list of selected entries in the first stage. The developed system is also capable to ensure that any two enrolled users do not have same name and/or password otherwise the system may give wrong results. The proposed integrated system has increased the accuracy of the system and at the same time overcomes the problem of non-enrollment of the user. The proposed system authenticates the persons in real time with an accuracy of 99.875%. Moreover, the integrated system also overcomes the problems of intra-class variation, noise and non-uniqueness (due to the presence of extra layer of security by the password).

In the second solution, two biometric, traits palm print and fingerprint have been combined at the score level. The fusion of these two biometric traits has been done using the Fuzzy logic. Three different sets of if-else rule have been formulated for low, medium and high security systems. In order to overcome the problem of non universality the rules for the low security system, have been formulated in such a way that if any of the inputs is with a reasonable score then the system accepts the claim of the user. With this type of arrangement 0% false rejection rate has been achieved but 0.75% cases of false acceptance has been reported. With the formulated rules of medium and high security false rejection rate increased to 1.61% and 2.88% respectively from the 0% for low security but false acceptance rate get reduced to 0.225% and 0% respectively.

In order to further decrease the possibility of false acceptance another layer of security in the form of speaker identification has been proposed in the very high security systems. Although with very high security system FRR of the system has increased but at the same time chance FAR has completely ruled out.

CHAPTER 6

Conclusions and Future Scope

The work presented in this thesis has been carried over a period and work on different modules has been carried out at different periods of time. The outcome of work has been presented in this chapter along with the future scope in this area.

6.1 Conclusions

The conclusions of the work are being presented in the point wise manner and are given below.

- The regional average thresholding is a better method than the global thresholding in case of Fingerprints.
- Thinning is an important pre-processing step in minutiae based automatic fingerprint authentication systems, as a good thinned image map can facilitate the minutiae extraction. The proposed algorithm improves the thinned image by reducing it to one pixel width and makes the image rotation independent. Single isolated pixels are also removed as they are not required in the final minutiae extraction stage. By using the Karnaugh map technique all the rules are simultaneously applied to each and every pixel which resulted in faster response as compared to look up table technique. The response time has been reduced by improving the window extraction for templates and by using the short circuit logical operators. An improved thinned image and overall reduction of about 40% in time has been achieved with the proposed methods.
- Crossing Number method is one of the most widely used Binarization based method for minutiae extraction but this method is not robust against false minutiae such as spikes and tends to register spike as minutiae. The new proposed method eliminates most of the false minutiae during the minutiae extraction stage because it uses genuine cases only. All these cases are solved to a minimized logical expression using a well known minimization technique of Karnaugh map. The proposed method

eliminates up to 10% false minutiae in the extraction stage, which remains with the crossing number method. It has also been observed that the while there is significant improvement in identification of ridge endings, only a few false ridge bifurcations are eliminated. Moreover, the proposed algorithm also takes care so that the boundary pixels should not be included in the list of minutiae.

- Rotation and translation between the reference and query images make it difficult to find the correspondence between the features (minutiae) of these two images. In the proposed Genetic Algorithm (GA) based relative alignment algorithm for the alignment of reference and query fingerprint image there is no need to find the reference core or delta point because reliable detection of these reference points is a difficult task. In order to find the accurate result all the three parameters x, y (translation) and θ (rotational) have to be optimized separately. The GA based algorithm was able to accurately find out the rotation, however because of optimization of all the parameters separately system becomes slow.
- This image-based fingerprint verification system provides a very simple and direct solution to the fingerprint matching problem. The system uses the much richer gray-level information of a fingerprint image. An image based fingerprint verification system has been developed and checked for the validity using the images from FVC2002/Db1_a database. The success rate of verification system is highly dependent on the threshold value and size of the template used for the learning stage. Smaller size learning image have lesser false rejection rate and higher false acceptance rate while larger size learning images have higher false rejection rate and lesser false acceptance rate. Moreover, higher the value of threshold, higher is the false rejection and lower is the false acceptance. So, a compromise has to be made between false acceptance and false rejection. The experimental results for different fingerprints with various learning image sizes reveals that a 100 x 100 learning image size for a threshold value of 700 (1000 being the perfect match) is a good compromise for false accept and false reject rate.
- It has been also been observed that the False Accept and False Reject Rate in most of the cases of enhanced images is high in comparison to the original image. This is due to the fact that although the enhancement of the images will improve the ridge valley

structure but richer gray level information is lost due to the enhancement process. So, preprocessing /enhancement of the images may be avoided in image based fingerprint authentication system.

- The proposed scheme of combining the biometric with the conventional method (speaker identification followed by password authentication) not only solved the problem of non uniqueness , interclass variation and noise but also overcome the problem of non enrollment of the user in the system which otherwise remains with the speaker identification system. Moreover, the results obtained indicate that the false reject rate can be reduced by extracting more entries during the identification stage.
- Fuzzy logic based technique used to fuse the two biometric traits at the score level is based on simple rules, which are very easy to apply and takes less time. In low security system in order to take care the problem non universality the rules are framed in such a manner that the matching of only one biometric is sufficient. In high security system the rules have been framed to overcome the problem of false acceptance. The addition of another biometric trait (voice) in the identification mode had further enhanced the security of the system. The advantage of using fuzzy logic is that there is the need to change the software part slightly when going from low security to high security system. While adding a biometric trait overcomes the problems of non uniqueness, intra-class variation etc., but it may add to user discomfort. So, a compromise has to be made between the security required and the user acceptance.

6.2 Future Scope

As discussed earlier the future belongs to the biometric based security systems for different applications such as physical access control, financial transactions etc.. So, the need is constantly felt to develop a biometric based technology with high success rate (Low FRR and FAR). While a significant improvement has been reported in this work for the development of different modules of single and multibiometric systems, still, we

believe that techniques proposed in this thesis can be further expanded and refined in the following ways.

1. The proposed K-map based minutiae extraction algorithm can take care of the spike (a false minutiae) in a 3×3 window but still post processing need to be performed to remove the false minutiae such as spur, hole, triangle etc. Rules may be formed in future to take care of these false minutiae by varying the window size from 3×3.

2. Although two speed up process have been incorporated for fitness evaluation function for alignment still it takes major time of minutiae based authentication system. Additional speed up steps may be incorporated to the present system to decrease the alignment time.

3. In future, a system using voice or speech can be thought off which will be independent of text and language.

4. In future, a biometric modality may be added to the system which will ensure the presence and aliveness of the user. e.g. ECG of the person may be incorporated as one of the biometric to ensure presence and aliveness of the user.

REFERENCES

1. E. Spinella, "Biometrics Scanning Technologies: Finger, Facial and Retinal Scanning", SANS Technology Institute, San Francisco, Dec., 2002.
2. N. Drakos, "An Introduction to Biometrics and Biometric Based Systems", Computer based Learning Unit, University of Leeds, 1998.
3. N. Ozkaya, S. Sagiroglu and A. Wani, "**An Intelligent Automatic Fingerprint Recognition System Design",** Proceedings of the 5th IEEE International Conference on Machine Learning and Applications, Orlando, Florida, pp. 231-238, 2006.
4. S. C. Dass and A. K. Jain, "Fingerprint-Based Recognition", *Technometrics*, vol. 49, no. 3, pp. 262-276, 2007.
5. P. Reid, "Biometric for Network Security", First Indian Reprint, Pearson Education, 2004.
6. http://www.spendonlife.com/guide/identity-theft-statistics
7. http://www.idsafety.net/901.R_IdentityFraudSurveyConsumerReport.pdf
8. http://www.globalsecurity.org/security/systems/biometrics-history.htm
9. http://www.questbiometrics.com/biometric-history.html
10. http://terrorism.about.com/od/issuestrends/tp/History-of-Biometrics.htm
11. http://www.biometricgroup.com/Henry%20Fingerprint%20Classification.pdf
12. http://www.reachoutmichigan.org/funexperiments/agesubject/lessons/prints_ext.html
13. http://www.globalsecurity.org/security/systems/fingerprint.htm
14. http://ctl.ncsc.dni.us/biomet%20web/BMIris.html
15. http://userweb.cs.utexas.edu/users/boyer/bledsoe-memorial-resolution.pdf
16. J. D. Woodward, N. M. Orlans and P. T. Higgins, "Identity Assurance in the Information Age- Biometrics", McGraw Hill, New York, 2003.
17. L. Sirovich and M. Kirby, "Low-Dimensional Procedure for the Characterization of Human Faces", Journal of the Optical Society of America, A: Optics, Image Science and Vision, vol. 4, no. 3, pp. 519-524, March, 1987.
18. S. K. Im, H.M. Park, Y.W. Kim, S.C. Han, S.W. Kim and C.H. Kang, "An Biometric Identification System by Extracting Hand Vein Patterns", Journal of the Korean Physical Society, vol. 38, no. 3, pp. 268-272, 2001.
19. http://cogt.client.shareholder.com/ReleaseDetail.cfm?ReleaseID=145765

20. http://www.globalsecurity.org/security/systems/biometrics.htm
21. http://en.wikipedia.org/wiki/United_States_passport
22. http://en.wikipedia.org/wiki/Biometrics
23. C. Soutar, "Implementation of Biometric Systems-Security and Privacy Considerations", Information Security Technicial Report, vol. 7, no. 4, Dec., 2002.
24. S. Prabhakar, S. Pankanti and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security and Privacy, vol. 1, no. 2, pp. 33-42, 2003.
25. K. Upendra, S. Singh, V. Kumar and H. K. Verma, "Online Fingerprint Verification", Journal of Medical Engineering and Technology, vol. 31, no. 1, pp. 36-45, 2007.
26. G. S. Ng, X. Tong, X. Tang and D. Shi, "Adjacent Orientation Vector Based Fingerprint Minutiae System", Proceedings of 17th IEEE International Conference on Pattern Recognition, Singapore, pp. 528-531, 2004.
27. S. Huvanandana, C. Kim and J. N. Hwang, "Reliable and Fast Fingerprint Identification for Security Application", Proceedings of IEEE International Conference on Image Processing, Quebec, Canada, vol. 2, pp. 503-506, 2000.
28. Y. Chen, A. K. Jain and M. Demirkus, "Pores and Ridges: High-Resolution Fingerprint Matching using Level 3 Features", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 1, pp. 15-27, 2007.
29. C. Kant and R. Nath, "Reducing Process-Time for Fingerprint Identification System", International Journal of Biometrics and Bioinformatics, vol. 3, no. 1, pp. 1-9, 2009.
30. J. Feng, "Combining Minutiae Descriptor for Fingerprint Matching," Pattern Recognition, vol. 41, no. 1, pp. 342-352, 2008.
31. J. S. Mason and J. D. Brand, "The Role of Dynamics in Visual Speech Biometric", Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Orlando, Florida, pp. 142-147, 2002.
32. A. K. Jain, A. Ross and S. Pankanti, "A Proto type Hand Gemetry- based Verification System", 2nd International conference on Audio and Video based Biometric Personal Authentication, Washington, USA, pp. 166-171, 1999.
33. M. Cannon, M. Byrne, D. Cotter, P. Sham, C. Larkin and E. O'Callaghan, "Further Evidence for Anomalies in the Hand-prints of Patients with Schizophrenia: A Study of Secondary Creases", Schizophrenia Research, vol. 13, pp. 179-184, 1994.

34. A. Kong, D. Zhang and G. Lu, "A Study of Identical Twins Palmprint for Personal Verification", Pattern Recognition, vol. 39, no. 11, pp. 2149-2156, 2006.
35. http://www.biometricnewsportal.com/signature_biometrics.asp
36. **R. Guest, "**Age Dependency in Handwritten Dynamic Signature Verification Systems", Pattern Recognition Letters, vol. 27, no. 10, pp. 1098-1104, 2006.
37. http://www.biometrics.co.uk/signature_biometrics/
38. D. C. Leonard, A. P. Pons, and S. S. Asfour, "Realization of a Universal Patient Identifier for Electronic Medical Records through Biometric Technology", IEEE Transactions on Information Technology in Biomedicine, vol. 13, no. 4, pp. 494-500, 2009.
39. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1572236
40. G. Zayaraz, V. Vijayalakshmi and D. Jagadiswary, "Securing Biometric Authentication Using DNA Sequence and Naccache Stern Knapsack Cryptosystem", Proceedings of International Conference on Control, Automation, Communication and Energy Conservation, Tamilnadu, India, pp. 1- 4, June, 2009.
41. H. Saevanee and P. Bhattarakosol, "Authenticating User using Keystroke Dynamics and Finger Pressure", Proceedings of 6th IEEE Conference on Consumer Communications and Networking, Las Vegas, pp. 1-2, 2009.
42. M. Karnan and M. Akila, "Personal Authentication based on Keystroke Dynamics using Soft Computing Techniques", Proceedings of 2nd IEEE International Conference on Communication Software and Networks, Singapore, pp. 334-338, February, 2010.
43. M. Karnan and M. Akila, "Identity Authentication based on Keystroke Dynamics using Genetic Algorithm and Particle Swarm Optimization", Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, China, pp. 203-207, August, 2009.
44. I. Khan, "Vein Pattern Recognition - Biometrics Underneath the Skin" 7 Nov. 2006 http://www.frost.com/prod/servlet/market-insight-top.pag?docid=86268767
45. M. David, S. J. Horng, "A Study of Finger Vein Biometric for Personal Identification", International Symposium on Biometrics and Security Technologies, Islamabad, Pakistan, pp. 1-8, April, 2008.
46. A. Ross, A. K. Jain and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Special issue on Image and

Video based Biometric, vol. 14, no. 1, pp. 4-20, 2004.

47. S. Pankanti, S. Prabhakar and A.K. Jain, "On the Individuality of Fingerprints", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 24, no. 8, pp. 1010-1025, 2002.
48. http://www.interpol.int/public/Forensic/fingerprints/WorkingParties/IEEGFI/ieegfi.asp
49. A. K. Jain, S. Prabhakar and S. Pankanti, "On the Similarity of Identical Twin Fingerprints", Pattern Recognition, vol. 35, no. 8, pp. 2653-2663, 2002.
50. A.K. Jain and A. Ross, "Multibiometric Systems", Communications of ACM, Special issue on Multimodal Interfaces, vol. 47, no. 1, pp. 34-40, 2004.
51. http://www.onin.com/fp/fphistory.html
52. A. Moenssens, "Fingerprint Techniques", Chilton, London, 1971.
53. H. Cummins and R. Kennedy, "Purkinje's Observations (1823) on Finger prints and other Skin Features", The Journal of Criminal Law and Criminology, vol. 31, no. 3, pp. 343-356, 1940.
54. W. J. Herschel, "Skin Furrows of the Hand", Nature, vol. 23, pp. 76-76, 1880.
55. E. Keogh, "An overview of the Science of Fingerprints", Anil Aggarwal's Internet Journal of Forensic Medicine and Taxicology, pp. 2(1), 2001.
56. F. Galton, "Finger prints", McMillan, London, 1892.
57. E. Henry, "Classification and uses of Fingerprints", Routledge, London, 1900.
58. T. P. Chen, W. Y. Yau and X. Jiang, "Token-Based Fingerprint Authentication", Recent Patents on Computer Science, vol. 2, pp. 50-58, 2009.
59. http://www.biometrics.gov/Documents/FingerprintRec.pdf
60. R. C. Gonalez and R. E. Woods, "Digital Image Processing", Second Edition, Pearson Education, 2005.
61. A. M. Bazen and S. H. Gerez, "Directional Field Computation for Fingerprints based on the Principal Component Analysis of Local Gradients", Proceedings of 11th Annual Workshop on Circuits, Systems and Signal Processing, Veldhoven, Netherlands, pp. 1-7, November, 2000.
62. K. Nandakumar and A. K. Jain, "Local Correlation-based Fingerprint Matching", Proceedings of Indian Conference on Computer Vision, Graphics & Image Processing, pp. 1-6, Kolkata, December, 2004.

63. A. Cavusoglu and S. Gorgunoglu, “A Robust Correlation based Fingerprint Matching Algorithm for Verification”, Journal of Applied Sciences, vol. 7, no. 21, pp. 3286-3291, 2007.

64. Z. Ouyang, J. Feng, F. Su and A. Cai, “Fingerprint Matching with Rotation Descriptor Texture Features”, Proceedings of 18th International Conference on Pattern Recognition, Hong Kong, vol. 4, pp. 417-420, Aug., 2006.

65. K. Ito, A. Morita, T. Aoki, T. Higuchi, H. Nakajima, and K. Kobayashi, “A Fingerprint Recognition Algorithm using Phase-based Image Matching for Low Quality Finger prints”, Proceedings of IEEE International Conference on Image Processing, Genoa, Italy, vol. 2, pp. 33-36, September, 2005.

66. J. Zhang, Z. Ou and H. Wei, “Fingerprint Matching using Phase only Correlation and Fourier-Mellin Transforms”, Proceedings of the 6th International Conference on Intelligent Systems Design and Applications, Jian, China, pp. 379-383, 2006.

67. D. Maio and D. Maltoni, “Direct Gray-Scale Minutiae Detection in Fingerprints”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.19, no.1, pp. 27-40, 1997.

68. O. Gorman and J. V. Nickerson, “An approach to Fingerprint Filter Design”, Pattern Recognition, vol. 22, no. 1, pp. 29-38, 1989.

69. B. G. Sherlock, D. M. Monro and K. Millard, “Fingerprint Enhancement by Directional Fourier Filtering”, Proceedings of IEE Vision, Image and Signal Processing, vol. 141, no. 2, pp. 87-94, 1994.

70. L. Hong, Y. Wan and A. K. Jain, “Fingerprint Image Enhancement: Algorithms and Performance Evaluation”, IEEE Transactions on Pattern Analysis Machine Intelligence, vol. 20, no. 8, pp. 777-789, 1998.

71. J. Yang, L. Liu, T. Jiang and Y. Fan, “A Modified Gabor Filter Design Method for Fingerprint Image Enhancement”, Pattern Recognition Letters, vol. 24, no. 12, pp. 1805-1817, 2003.

72. W. Wang , L. Jianwei, F. Huang and H. Feng, **“**Design and Implementation of Log-Gabor Filter in Fingerprint Image Enhancement”, Pattern Recognition Letters, vol. 29, no. 3, pp. 301-308, 2008.

73. W. Jang, D. Park, D. Lee and S. Kim, “Fingerprint Image Enhancement Based on Half Gabor Filter”, International Conference on Biometrics, Hong Kong, pp. 258-264, 2006.

74. A. J. Wills and L. Myers, “A Cost Effective Fingerprint Recognition system for use with Low Quality Prints and Damaged Fingertips”, Pattern Recognition, vol. 34, no. 2, pp. 255-270, 2001.

75. S. Chikkerur, A. N. Cartright and V. Govindaraju, “Fingerprint Enhancement using STFT Analysis”, Pattern Recognition, vol. 40, no. 1, pp. 198-211, 2007.

76. C. T. Hsieh, E. Lai and Y. C. Wan “An Effective Algorithm for Fingerprint Image Enhancement based on Wavelet Transform”, Pattern Recognition, vol. 36, no. 2, pp. 303-312, 2003.

77. W. P. Zhang, Y. Vantang and X. You, “Fingerprint Enhancement using Wavelet Transform Combined with Gabor Filter”, Journal of Pattern Recognition and Artificial Intelligence, vol. 18, pp. 1391-1406, 2004.

78. B.M. Mehtre, N.N. Murthy, S. Kapoor and B. Chatterjee, “Segmentation of Fingerprint Images using the Directional Image”, Pattern Recognition, vol. 20, no. 4, pp. 429-435, 1987.

79. B. M. Mehtre and B. Chatterjee, “Segmentation of Fingerprint Images – A Composite Method”, Pattern Recognition, vol. 22, no. 4, pp. 381-385, 1989.

80. N. Ratha, S. Chen and A. Jain, “Adaptive Flow Orientation based Feature Extraction in Fingerprint Images”, Pattern Recognition, vol. 28, pp. 1657-1672, 1995.

81. L. Shen, A. Kot and W. M. Koo, ”Quality Measures of Fingerprint Images”, Proceedings of 3rd International Conference on Audio and Video Based Biometric Person Authentication, Halmstad, Sweden, pp. 266-271, 2001.

82. A. M. Bazen and S. H. Gerez, “Segmentation of Fingerprint Images”, Proceedings of Workshop on Circuits, Systems and Signal Processing, Veldhoven, Netherlands, pp. 276-280, Nov., 2001.

83. X. J. Chen, J. Tian, J. G. Cheng, X. Yang, “Segmentation of Fingerprint Images using Linear Classifier”, EURASIP Journal on Applied Signal Processing, pp. 480-494, 2004.

84. S. Klein, A. Bazen, R. Veldhuis, “Fingerprint Image Segmentation based on Hidden Markov Models”, Proceedings of 13th Annual Workshop on Circuits, Systems and Signal

Processing, Veldhoven, Netherlands, pp. 310-318, Nov., 2002.

85. R.C. Gonzalez and R. E. Woods, "Digital Image Processing", Pearson Education, New Delhi, 2005.
86. R. M. Stock and C.W. Swonger, "Development and Evaluation of a Reader of Fingerprint Minutiae", Tech. Report: No. XM-2478-X-1:13-17, Cornell Aeronautical Laboratory, 1969.
87. B. Moayer and K. Fu, "A Tree System Approach for Fingerprint Pattern Recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 8, no. 3, 376-388, 1986.
88. Q. Xiao and H. Raafat, "Combining Statistical and Structural Information for Fingerprint Image Processing Classification and Identification", Pattern Recognition: Architectures, Algorithms and Applications, pp. 335-354, 1991.
89. M. R. Verma, A. K. Majumdar and B. Chatterjee, "Edge Detection in Fingerprints", Pattern Recognition, vol. 20, pp. 513-523, 1987.
90. N. K. Ratha, S. Y. Chen, and A. K. Jain, "Adaptive Flow Orientation-based Feature Extraction in Fingerprint Images", Pattern Recognition, vol. 28, no. 11, pp. 1657-1672, 1995.
91. I. Emiroglu and M. B. A. Khan, "Preprocessing of Fingerprint Images", Proceedings of European Conference on Security and Detection, London, UK, pp. 147-151, April, 1997.
92. A. S. Abutaleb and M. Kamel, "A Genetic Algorithm for the Estimation of Ridges in Fingerprints", IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1134-1138, 1999.
93. L. Dong and G. Yu, "An Optimization-based approach to Image Binarization", Proceedings of the 4th International Conference on Computer and Information Technology, Wuhan, China, pp. 165-170, Sept., 2004.
94. V. Onnia and M. Tico, "Adaptive Binarization method for Fingerprint Images", Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Toulouse, France, vol. 4, pp. 3692-3695, Sept., 2002.
95. F. Kheiri, S. Samavi and N. Karimi, "A New Pipeline Design for Binarization and Thinning of Fingerprint Images", Proceedings of the Canadian Conference on Electrical and Computer Engineering, Saskatoon, Sask., Canada, pp. 2013-2016, May, 2005.

96. Y. Zhang and Q. Xiao, “An Optimized Approach for Fingerprint Binarization”, Proceedings of the International Joint Conference on Neural Networks, Vancouver, BC, Canada, pp. 391-395, July, 2006.

97. C. Wang and K. T. Wu, “Design of a Pixel Array Circuit for Thinning Process”, Proceedings of the IEEE International Symposium on Circuit and Systems, Montreal, Que., Canada, vol. 3, pp. 89-92, Sept., 2004.

98. N. H. Han, C. W. La and P. K. Rhee, “An Efficient Fully Parallel Thinning Algorithm”, Proceedings of IEEE International Conference on Document Analysis and Recognition, Ulm, Germany, vol. 1, pp. 137-141, Aug., 1997.

99. B. K Jang and R. T. Chin, “One Pass Parallel Thinning: Analysis, Properties and Quantitative Evaluation”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 14, no. 11, pp. 1129-1140, 1992.

100. A. Datta and S. K. Parui, “A Robust Parallel Thinning Algorithm for Binary Images”, Pattern Recognition, vol. 27, no. 9, pp. 1181-1192, 1994.

101. Y. Y. Zhang and P. S. P. Wang, “A Parallel Thinning Algorithm with Two-Sub Iteration that Generates One Pixel Wide Skeletons”, Proceedings of the IEEE Conference on Pattern Recognition, Vienna , Austria, vol. 4, pp. 457- 461, Aug., 1996.

102. M. Ahmed and R. Ward, “A Rotation Invariant Rule based Thinning Algorithm for Character Recognition”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 12, pp. 1672-1678, 2002.

103. L. Huang, G. Wan and C. Liu, “An Improved Parallel Thinning Algorithm”, Proceedings of the 7th International Conference on Document Analysis and Recognition, Washington, DC, USA, pp.780-783, 2003.

104. J. Luping , Y. Zhang , S. Lifeng and P. Xiaorong, “Binary Fingerprint Image Thinning using Template-based PCNNs”, IEEE Transactions on Systems, Man and Cybernetics, vol. 37, no. 5, pp. 1407-1413, 2007.

105. M. Leung, W. Engeler and P. Frank, “Fingerprint Image Processing using Neural Network”, Proceedings of the IEEE Region 10th Conference on Computer and Communication Systems, Hong Kong, pp. 582-586, September, 1990.

106. X. Jiang, W. Y. Yau and W. Ser, "Detecting the Fingerprint Minutiae by Adaptive Tracking the Gray Level Ridge", Pattern Recognition, vol. 34, no. 5, pp. 999-1013, 2001.

107. J. Liu, Z. Huang and K. Chan, "Direct Minutiae Extraction from Gray Level Fingerprint Image by Relationship Examination", Proceedings of the International Conference on Image Processing, Vancouver, BC, Canada, vol. 2, pp. 427-430, Sept., 2000.

108. K. Nilsson and J. Bigun, "Using Linear Symmetry Features as a Preprocessing Step for Fingerprint Images", Proceedings of the 3rd International Conference on Audio and Video based Biometric Person Authentication, Halmstad, Sweden, pp. 247-252, June, 2001.

109. F. Zhao and X. Tang, "Preprocessing and Postprocessing for Skeleton based Fingerprint Minutiae Extraction", Pattern Recognition, vol. 40, no. 4, pp.1270-1281, 2007.

110. A. Farina, Z. M. Kovács-Vajna and A. Leone, "Fingerprint Minutiae Extraction from Skeletonized Binary Images", Pattern Recognition, vol. 32, no. 5, pp. 877–889, 1999.

111. B. M. Mehtre, "Fingerprint Image Analysis for Automatic Identification", Machine Vision Applications, vol. 6, pp. 124–139, 1993.

112. S. A. Sudiro, M. Paindavoine and M. Kusuma, "Simple Fingerprint Minutiae Extraction Algorithm using Crossing Number on Valley Structure", IEEE Workshop on Automatic Identification Advanced Technologies, Alghero, Italy, pp. 41-44, 2007.

113. J. H. Wegstein, "An Automated Fingerprint Identification System", U.S. Government Publication, Washington, DC: U.S. Dept. of Commerce, National Bureau of Standards, 1982.

114. A. M. Bazen and S. H. Gerez, "Systematic Methods for the Computation of the Directional Fields and Singular Points of Fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 7, pp. 905-919, 2002.

115. A.K. Jain, L. Hong, S. Pankanti and R. Bolle, " An Identity Authentication System using Fingerprints", Proceedings of IEEE, vol. 85, no. 9, pp.1365-1388, 1997.

116. X. Luo, and J. Tian, "Knowledge Based Fingerprint Image Enhancement", Proceedings of 15th International Conference on Pattern Recognition, Barcelona , Spain, vol. 4, pp. 783-786, Aug., 2000.

117. W. Zhang and Y. Wang, "Core-Based Structure Matching Algorithm of Fingerprint Verification", Proceedings of the 16th International Conference on Pattern Recognition, Quebec City, Canada , pp. 70-74, August, 2002.

118. J. Feng, Z. Ouyang and A. Cai, "Fingerprint Matching using Ridges", Pattern Recognition, vol. 39, no. 11, pp. 2131-2140, 2006.

119. C. Hu, J. Yin, E. Zhu, H. Chen and Y. Li, "Fingerprint Alignment using Special Ridges", Proceedings of 19th IEEE international conference on Pattern Recognition, Tampa, FL, pp. 1- 4, 2008.

120. Q. Zhao, D. Zhang, L. Zhang and N. Luo, "High Resolution Partial Fingerprint Alignment using Pore–Valley Descriptors", Pattern Recognition, vol. 43, pp. 1050-1061, 2010.

121. Z. Chen and C. H. Kuo, "A Topology based Matching Algorithm for Fingerprint Matching", Proceedings of IEEE 25th Annual International Conference on Security Technology, Taipei, Taiwan, pp. 84-87, 1991.

122. A. K. Jain, L. Hong, S. Pankanti and S. Prabhakar, "FingerCode: A Filter Bank for Fingerprint Representation and Matching", Proceedings of the IEEE Computer Vision and Pattern Recognition, vol. 2, Collins, USA, pp. 187-195,1999.

123. A. K. Jain, A. Ross and S. Prabhakar, "Fingerprint Matching using Minutiae and Texture Features", Proceedings of the IEEE International Conference on Image Processing, Florianopolis, Brazil, pp. 287-289, 2001.

124. S. Huvanandana, S. Malisuwan and J. N. Hwang, "A Hybrid System for Automatic Fingerprint Identification", Proceedings of the IEEE International Symposium on Circuits and Systems, Bangkok, Thailand, vol. 2, pp. 952-955, 2003.

125. C. Jia, M. Xei and Q. Li, "A Fingerprint Minutiae Matching Approach based on Vector Triangle and Ridge Structure", Proceedings of IEEE International Conference on Communications, Circuits and Systems, Chendu, China, vol. 2, pp. 871-875, 2004.

126. A. V. Ceguerra and I. Koprinska, "Integrating Local and Global Features in Automatic Fingerprint Verification", Proceedings of IEEE 16th International Conference on Pattern Recognition, Quebec, Canada, pp. 347-350, 2002.

127. P. Bhowmick and B. B. Bhattacharya, “Approximate Fingerprint Matching using Kd Tree”, Proceedings of the IEEE International Conference on Pattern Recognition, Cambridge, United Kingdom, pp. 544-547, 2004.
128. L. Hong and L. Jain , “Automatic Personal Identification by Integrating Faces and Fingerprints”, in Proceedings of Workshop on Automatic Identification, Advanced Technologies, pp. 15-18, 1997.
129. L. Hong and A. K. Jain, “Integrating Faces and Fingerprints for personal Identification”, IEEE Transactions on Pattern Analysis Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, 1998.
130. A. K. Jain, L. Hong and Y. Kulkarni, “F2id: A Personnal Identification System using Faces and Fingerprint”, Proceedings of 14th International Conference on Pattern Recognition, Brisbane, Qld. , Australia, pp. 1373-1375, Aug., 1998.
131. M. Indovina, U. Uludag, R. Snelick, A. Mink and A. K. Jain, “Multimodal Biometric Authentication methods: A COTS Approach,” Proceedings of Workshop on Multimodal User Authentication, Santa Barbara, CA, pp. 99-106, Dec. 2003.
132. R. Snelick, U. Uludag, A. Mink , M. Indovina and A. K. Jain, “Large-scale Evaluation of Multimodal Biometric Authentication using State of the Art system”, IEEE Transactions on Pattern Analysis Machine Intelligence, vol. 27, no. 3, pp. 450-455, 2005.
133. D. Bouchaffra and A. Amira, “Structural Hidden Markov Models for Biometrics: Fusion of Face and Fingerprint”, Pattern Recognition, vol. 41, no. 3, pp. 852-867, 2008.
134. T. Sim, S. Zhang, R. Janakiraman and S. Kumar, “Continuous Verification using Multimodal Biometrics”, IEEE Transactions on Pattern Analysis Machine Intelligence”, vol. 29, no. 4, pp. 687-700, 2007.
135. A. Patra and S. Dass, “Enhancing Decision Combination of Face and Fingerprint by Exploitation of Individual Classifier Space: An Approach to Multi-modal Biometry”, Pattern Recognition, vol. 41, no. 7, pp. 2298-2308, 2008.
136. A. K. Jain, L. Hong and Y. Kulkarni, “A Multimodal Biometrics System using Fingerprint, Face and Speech”, Proceedings of 2nd International Conference on Audio-and Video-based Biometric Person Authentication, Washington D. C., U. S. A., pp. 182-187, March, 1999.

137. A. Ross, A. K. Jain and J. Qian, "Information Fusion in Biometrics", Proceedings of 3rd International Conference on Audio-and Video-based Biometric Person Authentication", Sweden, pp. 354-359, June, 2001.

138. A. Ross and A. K. Jain, "Information Fusion in Biometrics", Pattern Recognition letters, vol. 24, no. 13, pp. 2115-2125, 2003.

139. J. F. Angular, D. G. Romero, J. O. Garcia and J. Gonzalez, "Bayesian Adaptation for User-dependent Multimodal Biometric Authentication", Pattern Recognition, vol. 38, no. 8, pp. 1317-1319, 2005.

140. K. A. Toh, W. Xiong, W. Y. Yau and X. Jiang, "Combining Fingerprint and Hand Geometry Verification Decisions", Proceedings of 4th International Conference on Audio and Video based Biometric Person Authentication, Guildford, UK , pp. 688-696, June, 2003.

141. Y. Wang, Y. Wang and T. Tan, "Combining Fingerprint and Voiceprint Biometrics for Identity Verification: An Experimental Comparison", Proceedings of Ist International Conference on Biometric Authentication, Hong Kong, China, pp. 663-670, July, 2004.

142. K. A. Toh and W. Y. Yau, "Combination of Hyperbolic Functions for Multimodal Biometrics Data Fusion", IEEE Transaction on Systems, Man and Cybernetics, vol. 34, no. 1, pp. 85-94, 2004.

143. K. A. Toh and W. Y. Yau, "Fingerprint and Speaker Verification Decisions Fusion using a Functional Link Network", IEEE Transaction on Systems, Man, and Cybernetics, vol. 35, no 3, pp. 357-370, 2005.

144. A. K. Jain, S. C. Dass and K. Nandkumar, "Can Soft Biometric Traits Assist user Recognition?", Proceedings of SPIE Conference on Biometric Technology for Human Identification, Orlando, FL, vol. 5404, pp. 561-572, April, 2004.

145. A. K. Jain, S. C. Dass and K. Nandkumar, "Soft Biometric Traits for Personal Recognition Systems", Proceedings of Ist International Conference on Biometric Authentication, Hong Kong, China, pp. 731-738, July, 2004.

146. H. Ailisto, E. Vildjiounaite, M. Lindholm, S. M. Makela and J. Peltola, "Soft Biometrics-Combining Body Weight and Fat Measurements with Fingerprint Biometrics," Pattern Recognition Letters, vol. 27, no. 5, pp. 325-334, 2006.

147. A. K. Jain, K. Nanadakumar, X. Lu and U. Park, "Integrating Faces, Fingerprints and Soft Biometric Traits for user Recognition", Proceedings of Workshop on Biometric Authentication, Prague, pp. 259-269, May, 2004.

148. S. Ribaric and I. Fratric, "A Biometric Identification System based on Eigen palm and Eigenfinger Features", IEEE Transactions on Pattern Analysis Machine Intelligence, vol. 27, no. 11, pp. 1698-1709, 2005.

149. A. Kumar and D. Zhang, "Combining Fingerprint, Palmprint and Hand-shape for user Authentication", Proceedings of 18th International Conference on Pattern Recognition, Hong Kong, China, vol. 4, pp. 549-552, Aug., 2006.

150. S. S. Iyengar, L. Prasad and H. Min, "Advances in Distributed Sensor Technology", Prentice Hall, 1995.

151. K. Choi, H. Choi, and J. Kim, "Fingerprint Mosaicking by Rolling and Sliding", Proceedings of 5th International Conference on Audio and Video based Biometric Person Authentication, Rye Brook, USA, pp. 260-269, July, 2005.

152. A. K. Jain and A. Ross, "Fingerprint Mosaicking", IEEE International Conference on Acoustics, Speech, and Signal Processing, Orlando, USA, vol. 4, pp. 4064-4067, May, 2002.

153. Y. S. Moon, H. W. Yeung, K. C. Chan and S. O. Chan, "Template Synthesis and Image Mosaicking for Fingerprint Registration: An Experimental Study", IEEE International Conference on Acoustics, Speech, and Signal Processing, Montreal, Canada, vol. 5, pp. 409-412, May, 2004.

154. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Image Mosaicking for Rolled Fingerprint Construction", Proceedings of Fourteenth International Conference on Pattern Recognition, Brisbane, Australia, vol. 2, pp. 1651-1653, August, 1998.

155. Y. L. Zhang, J. Yang and H. Wu. "A Hybrid Swipe Fingerprint Mosaicking Scheme", Proceedings of Fifth International Conference on Audio and Video based Biometric Person Authentication, Rye Brook, USA, pp. 131-140, July, 2005.

156. A. Ross and R. Govindarajan, "Feature Level Fusion Using Hand and Face Biometrics", Proceedings of SPIE Conference on Biometric Technology for Human Identification II, Orlando, USA, vol. 5779, pp. 196-204, March, 2005.

157. A. Kumar and D. Zhang, “Personal Authentication using Multiple Palmprint Representation”, Pattern Recognition, vol. 38, no.10, pp. 1695-1704, 2005.

158. G. Feng, K. Dong, D. Hu, and D. Zhang, “When Faces are Combined with Palm- prints: A Novel Biometric Fusion Strategy”, First International Conference on Biometric Authentication, Hong Kong, China, pp. 701-707, July, 2004.

159. A. K. Jain and B. Chandrasekaran, “Dimensionality and Sample Size Considerations”, Handbook of Statistics, vol. 2, pp. 835-855, 1982.

160. S. Karanwal, D. Kumar and R. Maurya, “Score Level Fusion in Multimodal Biometric Systems”, Proceedings of the International Conference on Information Science and Applications, Chennai, India, pp. 403-406, Feb., 2010.

161. J. Daugman “Combining Multiple Biometrics”, 2000.
Available at http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html, 2000.

162. L. Lam and C. Y. Suen, “Application of Majority Voting to Pattern Recognition: An Analysis of its Behavior and Performance”, IEEE Transactions on Systems, Man, and Cybernetics, vol. 27, no. 5, pp. 553-568, 1997.

163. L. I. Kunchev, “Combining Pattern Classifiers - Methods and Algorithms”, Wiley, 2004.

164. Q. Xiao and H. Raafat, “Fingerprint Image Post processing: A Combined Statistical and Structural Approach”, Pattern Recognition, vol. 24, no.10, pp. 985–992, 1991.

165. D. C. D. Hung, “Enhancement and Feature Purification of Fingerprint Images”, Pattern Recognition, vol. 26, no. 11, pp. 1661-1671, 1993.

166. M. Tico and P. Kuosmanen, “An Algorithm for Fingerprint Image Postprocessing”, Proceedings of the 34th Asilomar Conference on Signals, Systems and Computers, vol. 2, pp. 1735-1739, November, 2000.

167. A. Tariq, M. U. Akram, S. Nasir, and R. Arshad, “Fingerprint Image Postprocessing using Windowing Technique”, Proceedings of International Conference on Image Analysis and Recognition, Portugal, pp. 915-924, June, 2008.

168. D. E. Goldberg, “Genetic Algorithms in Search, Optimization & machine Learning”, Pearson Education, 2006.

169. “Genetic Algorithm and Direct Search Toolbox Users Guide”, The Math Works, 2004.

170. J. Travis, “LabVIEW for Everyone”, second edition, Prentice Hall, New Jerssy, 2002.
171. http://zone.ni.com/devzone/cda/tut/p/id/3763
172. Z. M. Kovacs-Vajana, “A Fingerprint Verification System based on Triangular Matching and Dynamic Time Warping”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, pp. 1266-1276, 2000.
173. B. C. Nakra and K. K. Chaudhry, “Instrumentation, Measurement and Analysis”, Second Edition, Tata Mcgraw Hill Publishing Company Limited, New Delhi, 2005.
174. A. Lindoso, L. Entrena, C. López-Ongil and J. Liu, “Correlation-Based Fingerprint Matching using FPGAs”, Proceedings of IEEE International Conference on Field-Programmable Technology, Singapore, pp. 87-94, 2005.
175. "IMAQ Vision Concepts Manual", National Instruments Corporation, Austin, 2000.
176. S. Haykin and B. V. Veen, “Signals and Systems”, John Wiley and Sons, 1999.
177. A. R. Rao, “A Taxonomy of Texture Descriptions” Springer Verlag, 1990.
178. T. Mansfield and M. R. Greene, “Feasibility Study on the use of Biometrics in an Entitlement Scheme”, Center for Mathematic and Scientific Computing NPL, Teddington, Middlesex, version 3, pp. 1-38, February, 2003.
http://dematerialisedid.com/PDFs/feasibility_study031111_v2.pdf
179. P. M. Corby, T. Schleyer, H. Spallek, T. C. Hart, R. J. Weyant, A. L. Corby and W. A. Bretz, “Using Biometrics for Participant Identification in a Research Study: A Case Report”, Journal of the American Medical Informatics Association vol. 13 no. 2, pp. 233-235, 2006.
180. http://news.bbc.co.uk/2/hi/uk_news/politics/3693375.stm
181. M. Golfarelli, D. Maio and D. Maltoni, “On the Error-Reject Tradeoff in Biometric Verification Systems”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 786–796, 1997.
182. Y. Chen, S. C. Dass and A. K. Jain, “Fingerprint Quality Indices for Predicting Authentication Performance”, Proceedings of Fifth International Conference on Audio and Video-Based Biometric Person Authentication, New York, U.S.A., pp. 160-170, July, 2005.
183. A. Eriksson and P. Wretling, “How Flexible is Human Voice? A Case study of Mimicry”, Proceedings of European Conference on Speech Technology, Rhodes, pp. 1043-1046, 1997.

184. D. A. Black, “Forgery above a Genuine Signature”, Journal of Criminal Law, Criminology and Police Science, vol. 50, pp. 585-590, 1962.

185. W. Harrison “Suspect Documents- Their Scientific Examination”, Nelson Hall Publishers, 1981.

186. A. E. Rosenberg, “Automatic Speaker Verification: A Review”, Proceedings of IEEE, vol. 64, pp. 475-487, April, 1976.

187. J. M. Naik, L. Netsch and G. Doddington, “Speaker Verification over Long Distance Telephone Lines”, Proceedings of International conference on Acoustic, Speech Signal Processing, Glasgow, Scotland, pp. 524-527, 1989.

188. T. F. Quatieri, “Discrete Time Speech Signal Processing: Principles and Practice”, Pearson Education, 2001.

189. A. Gatherer and E. Auslander, “The Applications of Communications of Programmable DSPs in Mobile Communication”, Jhon – Wiley and Sons Ltd., 2001.

190. H. L. Lu, “Toward a High-Quality Singing Synthesizer with Vocal Texture Control”, Ph.D. thesis, Dept. of Electrical Engineering - Stanford University, Palo Alto, USA, July, 2002.

191. F. J Harris, “On the Use of Windows for Harmonic Analysis with the Discrete Fourier Transform”, Proceedings of the IEEE, vol. 66, pp. 66-67, 1978.

192. A. F. Souza and M. N. Souza, “Comparative Analysis of Speech Parameters for the Design of Speaker Verification Systems”, Proceedings of IEEE 23rd Annual EMBS International Conference, Istanbul, Turkey, pp. 2178-2181, 2001.

193. J. P. Campbell, “Speaker Recognition: A Tutorial”, Proceedings of IEEE, vol.85, no.9, Sep., 1997.

194. A. Kabir, S. Mohammad and M. Ahasan, “Vector Quantization in Text Dependent Automatic Speaker Recognition using Mel-frequency Cepstrum Coefficient”, Proceedings of 6th WSEAS International Conference on Circuits, Systems, Electronics, Control & Signal Processing, Cairo, Egypt, pp. 352-355, Dec., 2007.

195. H. B. Kekre and V. Kulkarni, “Speaker Identification by using Vector Quantization”, International Journal of Engineering Science and Technology, vol. 2, no.5, pp. 1325-1331, 2010.

196. T. Masuko, T. Hitotsumatsu, K. Tokuda and T. Kobayashi, “On the Security of HMM-

based Speaker Verification Systems against Imposture using Synthetic Speech", Proceedings of the European Conference on Speech Communication and Technology, Budapest, Hungary, vol. 3, pp. 1223-1226, September, 1999.

197. C. N. Hsu, H. C. Yu and B. H. Yang, "Speaker Verification Without Background Speaker Models", Proceedings of IEEE Conference on Acoustics, Speech, and Signal Processing, Hong Kong, pp. II-233-236, 2003.
198. D. A. Reynolds and R. C. Rose, "Robust Text-Independent Speaker Identification using Gaussian Mixture Speaker Models", IEEE Transactions on Speech and Audio Processing, pp.72-83, 1995.
199. S. Bhattacharyya, T. Srikanthan and P. Krishnamurthy, "Speaker Verification - A VLSI Perspective", Proceedings of 3rd International Symposium on Communication Systems, Networks and Digital Signal Processing, Staffordshire, UK, pp. 379-382, July, 2002.
200. R. O. Duda, P. E. Hart and D. G. Stork, "Pattern Classification", 2nd edition, John Wiley and Sons, New York, USA, 2001.
201. A. W. K. Kong and D. Zhang, "Competitive Coding Scheme for Palmprint Verification", Proceedings of 17th International Conference on Pattern Recognition, Cambridge UK, vol. 1, pp. 520-523, Aug., 2004.
202. D. Zhang, W. K. Kong, J. You and M. Wong, "On-line Palmprint Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 9, pp. 1041-1050, 2003.
203. C. C. Han, H. L. Cheng, C. L. Lin and K. C. Fan, "Personal Authentication using Palm-print Features", Pattern Recognition, vol. 36, no. 2, pp. 371-381, 2003.
204. W. Li, D. Zhang and Z. Xu, "Palmprint Identification by Fourier Transform", International Journal of Pattern Recognition and Artificial Intelligence, vol. 16, no. 4, pp. 417-432, 2002.
205. X. Wu, K. Wang and D. Zhang, "HMMs based Palmprint Identification", Lecture Notes in Computer Science, Springer, vol. 3072, pp. 775-781, 2004.
206. A. Kumar, D. C. M. Wong, H. C. Shen and A. K. Jain, "Personal Verification using Palmprint and Hand Geometry Biometric," Lecture Notes in Computer Science, Springer, pp. 668-678, 2003.
207. X. Wu, K. Wang and D. Zhang, "Line Feature Extraction and Matching in Palmprint", Proceedings of the 2nd International Conference on Image and Graphics, Hefei, China, pp.

583-590, Aug., 2002.

208. X. Wu, K. Wang and D. Zhang, "Fuzzy Direction Element Energy Feature based Palmprint Identification", Proceedings of 16th International Conference on Pattern Recognition, Quebec City, Canada, vol. 1, pp. 95-98, Aug., 2002.
209. M. R. Diaz, C. M. Travieso, J. B. Alonso and M. A. Ferrer, "Biometric System based in the Feature of Hand Palm", Proceedings of 38th Annual International Carnahan Conference on Security Technology, Albuquerque, NM, USA, pp. 136-139, Oct., 2004.
210. X. Wu, D. Zhang and K. Wang, "Fisherpalms based Palmprint Recognition", Pattern Recognition Letters, vol. 24, no. 15, pp. 2829-2838, 2003.
211. G. Lu, D. Zhang and K. Wang, "Palmprint Recognition using Eigenpalms Features", Pattern Recognition Letters, vol. 24, no. 9, pp. 1463-1467, 2003.
212. X. Y. Jing and D. Zhang, "A Face and Palmprint Recognition Approach based on Discriminant DCT Feature Extraction", IEEE Transactions on Systems, Man and Cybernetics Part B: Cybernetics, vol. 34, no. 6, pp. 2405-2415, 2004.
213. C. C. Han, H. L. Cheng, C. L. Lin and K. C. Fan, "Personal Authentication using Palm-print Features", Pattern Recognition, vol. 36, no. 2, pp. 371-381, 2003.
214. J. You, W. K. Kong, D. Zhang and K. H. Cheung, "On Hierarchical Palmprint Coding with Multiple Features for Personal Identification in Large Databases", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 2, pp. 234-243, 2004.
215. A. Kong, D. Zhang and M. Kamel, "Palmprint Identification using Feature-Level Fusion", Pattern Recognition, vol. 39, no. 3, pp. 478-487, 2006.
216. Z. Sun, T. Tan, Y. Wang and S. Z. Li, "Ordinal Palmprint Representation for Personal Identification", Proceedings of Conference on Computer Vision and Pattern Recognition, vol. 1, pp 279-284, 2005.
217. P. Hennings and B. V. K. V. Kumar, "Palmprint Recognition using Correlation Filter Classifiers", Proceedings of the 38th Asilomar Conference on Signal, Systems and Computers, vol. 1, pp. 567-571, June, 2004.
218. http://www.seattlerobotics.org/encoder/mar98/fuz/fl_part1.html
219. N. Sulaiman, Z. A. Obaid, M. H. Marhaban and M. N. Hamidon, "FPGA-Based Fuzzy Logic: Design and Applications – a Review", IACSIT International Journal of Engineering and Technology, vol.1, no.5, pp. 491-503, 2009.

220. http://www.seattlerobotics.org/encoder/mar98/fuz/fl_part2.html

221. H. Singh, J. Raj, G. Kaur and T. Meizler, "Image Fusion using Fuzzy Logic and Applications", Proceeding of the IEEE International Conference on Fuzzy Systems, Budapest, Hungary, vol. 1, pp.337-340, 2004.

222. V. B. Rao and H. Rao, **"C++ Neural Networks and Fuzzy Logic",** M & T Books, 1995.

223. T. J. Ross, "Fuzzy Logic with Engineering Applications", Second Edition, John Wiely & Sons, 2005.

224. S.N. Sivanandam, S. Sumathi and S.N. Deepa, "Introduction to Fuzzy Logic using MATLAB", Springer, 2007.

List of Research Papers Published and Presented

1. S. K. Singla and A. S. Arora, "Speaker Verification System Using LabVIEW", Institution of Electronics and Telecommunication Engineers Technical Review, vol. 24, no. 5, pp 403-412, 2007.
2. A. S. Arora and S. K. Singla, "Image Based Fingerprint Verification System using LabVIEW", Majeo International Journal of Science and Technology, vol.2, no.3, pp. 489-501,2008.
3. S. K. Singla and A. S. Arora, "An Improved and Efficient Thinning Algorithm for Fingerprints", Signal Processing and Pattern Recognition, Vol. 52, No. 2, pp.13-24, AMSE, FRANCE.
4. S. K. Singla and A. S. Arora "A Karnaugh Map Based Fingerprint Minutiae Extraction Method", Songklanakarin International Journal of Science and Technology, vol. 32, no. 3, pp. 247-254, 2010.
5. S. K. Singla and A. S. Arora "Optimizing the Rotation and Translation of Fingerprint Images using Genetic Algorithm", submitted to International Journal of Applied Artificial Intelligence, Taylor & Francis, Inc., Philadelphia.
6. S. K. Singla and A. S. Arora, "Integrating biometric with conventional techniques for user Authentication", submitted to ETRI Journal, Information, Telecommunications and Electronics, South Korea.
7. A. S. Arora and S. K. Singla, "Sensors for Fingerprint Technology", Proceeding of National Conference on Sensors, pp.122-124, TIET, Patiala, 2005.
8. S. K. Singla and A. S. Arora, " A Fingerprint Verification System", Proceeding of International Conference on Intelligent Systems and Networks, pp. 120-122, Kalwad, India, 2008.